(19) Евразийское патентное ведомство

(21) 202393359 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.01.24

(22) Дата подачи заявки
2022.05.23

(51) Int. Cl. ***G06Q 20/08*** (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/30 (2012.01)

(54) СИСТЕМА И СПОСОБ ОБЛЕГЧЕНИЯ ОСНОВАННЫХ НА ПРАВИЛАХ ЧАСТИЧНО ОНЛАЙН И ОФЛАЙН ПЛАТЕЖНЫХ ТРАНЗАКЦИЙ

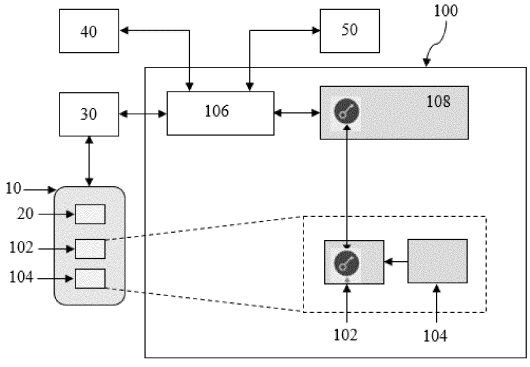
(31) **202121023338**
(32) **2021.05.25**
(33) **IN**
(86) **PCT/IB2022/054791**
(87) **WO 2022/249023 2022.12.01**

(71) Заявитель:
НЭШИОНАЛ ПЕЙМЕНТС КОРПОРЭЙШН ОФ ИНДИА (IN)

(72) Изобретатель:
Кхан Ариф, Дубей Ашутош, Гаурав Нишант, Палагири Сатиш (IN)

(74) Представитель:
Зуйков С.А. (RU)

(57) Настоящее изобретение раскрывает систему (100) и способ (200) облегчения зарегистрированным пользователям выполнять основанные на правилах частично онлайн и офлайн платежные транзакции. Инструмент PSP (20), установленный на электронном устройстве (10), связанном с зарегистрированным пользователем, выполняет доверенное приложение (104) в безопасной области хранения устройства (10). Доверенному приложению (104), инструменту PSP (20) и серверу PSP (30) предоставляют возможность осуществлять связь с механизмом аутентификации (108) и множеством серверов банковской системы (40, 50) через электронный коммутатор (106) для облегчения зарегистрированному пользователю регистрировать и создавать (204a) счет (UPI) lite единого платежного интерфейса; зачислять деньги (204b) на созданный счет с зарегистрированного финансового счета, при этом деньги хранят в виде балансовой стоимости в безопасной области хранения; и использовать балансовую стоимость (204c) для выполнения частично онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы (40, 50).



202393359 A1

202393359 A1

СИСТЕМА И СПОСОБ ОБЛЕГЧЕНИЯ ОСНОВАННЫХ НА ПРАВИЛАХ ЧАСТИЧНО-ОНЛАЙН И ОФЛАЙН ПЛАТЕЖНЫХ ТРАНЗАКЦИЙ

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Настоящее раскрытие в общем относится к платежным системам. Более конкретно, настоящее раскрытие относится к системе и способу облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций.

ОПРЕДЕЛЕНИЯ

Следующие термины, используемые в настоящем раскрытии, в общем будут иметь следующие значения, изложенные ниже, за исключением области, когда контекст, в котором их используют, указывает обратное.

Зарегистрированный пользователь – Термин «зарегистрированный пользователь» в дальнейшем относится к лицу, имеющему финансовый/банковский счет, и использующему электронную платежную систему на основе UPI для выполнения электронных платежных транзакций. Для использования электронной платежной системы на основе UPI, лицо имеет идентификатор UPI/виртуальный платежный адрес, привязанный к финансовому/банковскому счету. Зарегистрированный пользователь может быть плательщиком, т.е. лицом, которое желает отправлять/платить деньги, или может быть получателем платежа, т.е. лицом, которое получает/взимает деньги, используя электронную платежную систему на основе UPI.

Электронное устройство/ пользовательское устройство/ мобильное устройство – Термины «электронное устройство», «пользовательское устройство» и «мобильное устройство» в дальнейшем относятся к устройству, используемому зарегистрированным пользователем настоящего раскрытия, при этом пользовательское устройство включает, но не ограничивается этим, мобильный телефон, портативный компьютер, планшетный компьютер, iPad, КПК, ноутбук, нетбук, интеллектуальное устройство, смартфон, персональный компьютер, карманное устройство и т.п.

Платежные транзакции – Термин «платежные транзакции» в дальнейшем относится к финансовым, а также нефинансовым транзакциям. Финансовые транзакции содержат платежные транзакции клиент-клиент (P2P), клиент-счет (P2A) и клиент-платежный агент (P2M), основанные на запросе о взимании/выводе и запросе об оплате/передаче. Нефинансовые транзакции включают, но не ограничиваются этим, регистрацию мобильного банка, создание одноразового пароля (OTP), проверку баланса, установку или изменение PIN, регистрацию жалобы и проверку статуса транзакции.

Поставщик платежных услуг – Термин «поставщик платежных услуг (PSP)» в дальнейшем относится к интернет-банку, платежному банку, платежному инструменту с

предоплатой (PPI) или к любой другой организации, регулируемой централизовано или правительством, которой позволено привлекать клиентов и обеспечивать платежные (кредитные/дебетовые) услуги клиентам (физическим лицам или организациям). PSP обеспечивает соответствующие платежные инструменты/приложения, к которым могут быть допущены зарегистрированные пользователи на своих пользовательских устройствах для выполнения платежных транзакций. PSP обеспечивает инструмент для электронной обработки финансовых и нефинансовых транзакций.

Глобальный идентификатор или виртуальный платежный адрес или идентификатор UPI – Термины «глобальный идентификатор (GI)» или «виртуальный платежный адрес (идентификатор VPA/UPI)» или «идентификатор UPI (унифицированный платежный интерфейс)» в дальнейшем относятся к уникальному идентификатору, связанному с финансовым/банковским счетом зарегистрированного пользователя. Уникальный глобальный идентификатор (GI) или виртуальный платежный адрес (идентификатор VPA/UPI) используют для выполнения платежных транзакций. GI может включать мобильный номер, номер «Aadhaar», номер банковского счета или любой другой идентификатор, который может уникально и безопасно идентифицировать зарегистрированного пользователя настоящего раскрытия. Также идентификатор VPA/UPI может быть создан зарегистрированным пользователем для выполнения платежных транзакций. Подразумевают, что термин «глобальный идентификатор», используемый в настоящем документе, включает GI, VPA, а также идентификатор UPI.

Инструмент поставщика платежных услуг – Термин «инструмент поставщика платежных услуг (инструмент PSP)» в дальнейшем относится к приложению или инструменту, обеспечиваемому каждым PSP. Инструмент PSP может быть обеспечен на веб-портале или в магазине игр, и/или в мобильном интернете, или посредством других средств для обеспечения зарегистрированных пользователей интерфейсом с UPI через PSP.

Сервер унифицированного платежного интерфейса (UPI)/механизм аутентификации – Термин «сервер UPI»/«механизм аутентификации» в дальнейшем относится к центральной системе, которая облегчает взаимодействие между множеством PSP и банками (т.е., серверами банковской системы) для выполнения финансовых и нефинансовых транзакций.

Общая библиотека или доверенное приложение – Термины «общая библиотека» или «доверенное приложение» в дальнейшем относятся к авторизованному безопасному программному обеспечению, которое выполняют в безопасной среде в устройстве, и которое может быть выполнено только внедрением защищенного аутентифицированного кода, конфиденциальности, подлинности, приватности, целостности системы и прав

доступа к данным. Это улучшенная версия решения шифрования PIN, которая позволяет сохранять в себе значение, называемое «запасная стоимость» или «балансовая стоимость». Эта сумма будет иметь базовый актив, который будет защищен банком пользователя. Общая библиотека также хранит конфиденциальные учетные данные, такие как PIN, пароли, биометрию и т.д. Сведения об аутентификации собирают и зашифровывают внутри общей библиотеки. PSP не хранит зашифрованные учетные данные в каком-либо постоянном хранилище. PSP не собирает аутентификационные учетные данные эмитента вне общей библиотеки.

Запасная стоимость или балансовая стоимость – Термины «запасная стоимость» или «балансовая стоимость» в дальнейшем относятся к виртуальной форме суммы, базовый актив которой располагается в банке пользователя. Запасная/балансовая стоимость аналогична токену или цифровому активу, и имеет информацию о стоимости актива, владельце актива, эмитенте и дереве Меркла последних нескольких транзакций. Запасная стоимость позволяет осуществлять «товарные транзакции денежных средств/предварительно одобренные транзакции» из общей библиотеки.

Механизм аутентификации – Термин «механизм аутентификации» в дальнейшем относится к компоненту в пределах центральной системы, который будет подтверждать целостность частично-онлайн и офлайн транзакций и обеспечивать ответ в общую библиотеку на разрешение дополнительных таких транзакций. Механизм авторизации будет также хранить копию самых последних балансов на случай пользовательских сценариев, таких как восстановление баланса из-за повреждения/утери/замены устройства.

Идентификационный номер – Термин «идентификационный номер» в дальнейшем относится к событию создания учетной записи службы lite в механизме аутентификации, которая указывает уникальную запасную стоимость, находящуюся в безопасной области хранения.

Криптограмма – Термин «криптограмма» в дальнейшем относится к задаче, которая состоит из короткого фрагмента зашифрованного текста.

Криптограмма запроса авторизации (ARQC) – ARQC относится к хэшу, создаваемому общей библиотекой посредством персональных ключей для передачи сведений о транзакции в механизм аутентификации. Без ARQC транзакции не могут быть инициированы.

Криптограмма ответа авторизации (ARPC) – ARPC представляет собой код ответа, создаваемый механизмом аутентификации при получении и подтверждении ARQC. Механизм аутентификации расшифровывает транзакцию посредством открытых ключей, подтверждает сведения, отправленные общей библиотекой, и создает ARPC при успешном

подтверждении.

Частично-онлайн транзакция – Выражение «частично-онлайн транзакция» в дальнейшем относится к основанным на правилах транзакциям на небольшие суммы, выполняемым посредством системы и способа настоящего раскрытия, не затрагивая банковские серверы.

Онлайн-транзакция – Выражение «онлайн-транзакция» в дальнейшем относится к транзакциям на основе UPI, выполняемым посредством инструмента PSP, и проверяемым на подлинность посредством двухфакторной аутентификации с помощью серверов банковской системы эмитента.

Офлайн-транзакция – Выражение «офлайн-транзакция» в дальнейшем относится к основанным на правилах транзакциям, выполняемым без какого-либо соединения с данными или какой-либо связи с серверами PSP.

Элемент безопасности (SE) – Термин «элемент безопасности» или «SE» относится к большой интегральной схеме микропроцессора, которая может хранить конфиденциальные данные и запускать безопасные приложения, такие как платежные приложения. SE действует в качестве хранилища, защищающего приложения и данные, хранящиеся внутри, от атак вредоносных программ, которые типичны для хоста (т.е. операционной системы устройства).

Доверенная среда выполнения (TEE) - Термин «доверенная среда выполнения» или «TEE» представляет собой безопасную область главного процессора, которая гарантирует защиту кода и данных, загруженных внутрь, в отношении конфиденциальности и целостности.

Средство связи – Термин “средство связи” в дальнейшем относится к средству для передачи и получения электронных данных. Средства связи могут включать, например, Интернет, всемирную компьютерную сеть, интранет, кабель (включающий волоконно-оптический кабель), магнитные связи, электромагнитные связи (включающие радиочастотную, микроволновую и инфракрасную связи) и электронные связи. Средства беспроводной связи могут поддерживать различные сетевые протоколы и технологии беспроводной связи, такие как ближняя бесконтактная связь (NFC), Wi-Fi, Bluetooth, 4G Long Term Evolution (LTE), кодовое разделение каналов с многостанционным доступом (CDMA), универсальная система мобильной связи (UMTS) и глобальная система мобильной связи (GSM)

УРОВЕНЬ ТЕХНИКИ

Справочная информация в настоящем документе ниже относится к настоящему раскрытию, но не обязательно является известным уровнем техники.

В последние несколько лет, унифицированный платежный интерфейс (UPI) стал одним из приоритетных выборов для клиентов при выполнении розничных платежей. Возможность выполнять платежи посредством смартфонов в 2-3 клика, обеспечила повышенное удобство конечным пользователям. Однако количество платежных транзакций на основе UPI увеличилось экспоненциально, что привело к увеличению нагрузки на коммутатор эмитента и на серверы банков и поставщиков платежных услуг (PSP). Дополнительно, инфраструктура PSP, способная поддерживать такое большое количество транзакций и обеспечивать надежность с точки зрения показателя успешности, снизилась за несколько последних месяцев.

В дополнение к вышеизложенному, традиционные платежные транзакции на основе мобильных устройств требуют от пользователей обеспечивать конфиденциальную информацию, такую как UPI PIN, пароль или MPIN, для выполнения транзакций на небольшие суммы. Это увеличивает время, требуемое для обработки платежных транзакций на небольшие суммы, а также приводит к онлайн-подтверждению PIN для всех транзакций в банке, тем самым создавая высокую нагрузку на банковские серверы, что нежелательно.

Для решения вышеупомянутых проблем традиционных платежных решений, существует необходимость в системе и способе, которые облегчают основанные на правилах, частично-онлайн и офлайн платежные транзакции с низкой стоимостью, не затрагивая банковские серверы.

ЗАДАЧИ

Некоторые из задач настоящего раскрытия, которые по меньшей мере удовлетворяют один вариант выполнения настоящего документа, следующие:

Задачей настоящего раскрытия является устранение одной или нескольких проблем известного уровня техники или по меньшей мере обеспечение приемлемой альтернативы.

Одна задача настоящего раскрытия заключается в том, чтобы обеспечить систему и способ облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций.

Еще одна задача настоящего раскрытия заключается в том, чтобы обеспечить систему для облегчения транзакций на небольшие суммы, не требуя от пользователей раскрывать конфиденциальную информацию, такую как PIN или пароли.

Еще одна задача настоящего раскрытия заключается в том, чтобы обеспечить систему для облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций, которая уменьшает нагрузку по обработке на коммутатор эмитента, поставщиков платежных услуг и на серверы банковской системы.

Еще одна задача настоящего раскрытия заключается в том, чтобы обеспечить систему, которая облегчает основанные на правилах транзакции на небольшие суммы, не затрагивая банковские серверы.

Еще одна задача настоящего раскрытия заключается в том, чтобы обеспечить платежную систему для облегчения частично-онлайн и офлайн платежей, которые являются высокобезопасными.

Еще одна задача настоящего раскрытия заключается в том, чтобы обеспечить систему, которая предоставляет возможность зарегистрированным пользователям выполнять платежные транзакции в один клик.

Другие задачи и преимущества настоящего раскрытия станут более очевидными из следующего описания, при прочтении в сочетании с сопровождающими фигурами, которые не предназначены для ограничения объема настоящего раскрытия.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Настоящее раскрытие предусматривает способ облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн и офлайн платежные транзакции. Каждый из зарегистрированных пользователей имеет один или несколько инструментов поставщиков платежных услуг (PSP), установленных на их электронных устройствах. Каждый инструмент PSP размещен сервером PSP. Каждый из зарегистрированных пользователей имеет финансовый счет, связанный с уникальным многосимвольным PIN и глобальным идентификатором. Способ содержит следующие этапы, на которых

- выполняют, инструментом PSP, установленным на электронном устройстве, связанном с зарегистрированным пользователем, доверенное приложение в безопасной области хранения электронного устройства;

- предоставляют возможность, через центральный электронный коммутатор, доверенному приложению, инструменту PSP и серверу PSP связываться с механизмом аутентификации и множеством серверов банковской системы для предоставления возможности зарегистрированному пользователю регистрировать и создавать счет lite единого платежного интерфейса (UPI) для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций; зачислять деньги на созданный счет UPI lite с зарегистрированного финансового счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения; и использовать балансовую стоимость для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы.

В одном варианте выполнения этап предоставления возможности

зарегистрированному пользователю регистрировать и создавать счет UPI lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций, содержит этапы, на которых

i. получают, инструментом PSP, команду предоставления возможности услуги от зарегистрированного пользователя через интерфейс инструмента PSP, при этом команда предоставления возможности услуги содержит сведения о финансовом счете, к которому должна быть предоставлена возможность выполнения частично-онлайн и офлайн транзакций;

ii. создают, инструментом PSP, запрос на вызов открытого ключа при получении команды предоставления возможности услуги, и отправляют запрос на вызов созданного открытого ключа в доверенное приложение;

iii. создают, доверенным приложением, пару персональный (Ps) - открытый (Pk) ключ в пределах безопасной области хранения электронного устройства при получении запроса на вызов открытого ключа от инструмента PSP;

iv. отправляют, доверенным приложением, открытый ключ из созданной пары персональный-открытый ключ в инструмент PSP;

v. создают, инструментом PSP, запрос о списке ключей при получении открытого ключа, при этом запрос списка ключей содержит открытый ключ;

vi. передают, инструментом PSP, созданный запрос о списке ключей в электронный коммутатор через сервер PSP, связанный с инструмент PSP;

vii. осуществляют маршрутизацию, электронным коммутатором, запроса о списке ключей, получаемого с сервера PSP, в механизм аутентификации;

viii. открывают, механизмом аутентификации, счет UPI lite для зарегистрированного пользователя созданием цифрового сертификата (DC-Pk) посредством открытого ключа, и обновляют запрос о предоставлении возможности услуги с помощью уникального номера счета lite, при этом цифровой сертификат (Pk) и открытый ключ снабжены механизмом аутентификации для аутентификации будущих частично-онлайн или офлайн транзакций, инициируемых с электронного устройства;

ix. создают, механизмом аутентификации, успешный ответ о списке ключей при успешном открытии счета UPI lite и сохранении открытого ключа; и

x. передают, механизмом аутентификации, успешный ответ о списке ключей в инструмент PSP через электронный коммутатор и сервер PSP для уведомления зарегистрированного пользователя об успешном предоставлении возможности услуги для соответствующего финансового счета.

В одном варианте выполнения этап предоставления возможности

зарегистрированному пользователю зачислять деньги на созданный счет UPI lite с зарегистрированного финансового счета:

i. создают, инструментом PSP, напоминание о вводе PIN и суммы в интерфейсе инструмента PSP для извлечения многосимвольного PIN, и суммы пополнения от зарегистрированного пользователя для зачисления суммы на созданный счет UPI lite;

ii. получают, инструментом PSP, многосимвольный PIN и сумму пополнения через интерфейс инструмента PSP;

iii. напоминают, доверенным приложением, зарегистрированному пользователю выполнить подтверждение первого уровня реализацией сканирования устройством отпечатка пальца;

iv. создают, доверенным приложением, первый блок учетных данных, содержащий многосимвольный PIN, и второй блок учетных данных, содержащий первую криптограмму запроса авторизации (ARQC), после выполнения множества заранее определенных проверок;

v. получают, инструментом PSP, созданный первый и второй блок учетных данных от доверенного приложения;

vi. инициируют, инструментом PSP, запрос на зачисление денег в сервер PSP, при этом запрос на зачисление денег содержит первый и второй блок учетных данных;

vii. отправляют, сервером PSP, запрос на зачисление денег в механизм аутентификации через электронный коммутатор;

viii. проверяют подлинность, механизмом аутентификации, запроса сервиса предоставления возможности услуги первой ARQC, при получении запроса на зачисление денег;

ix. пересылают, электронным коммутатором, запрос на зачисление денег на сервер банковской системы эмитента, связанный с финансовым счетом зарегистрированного пользователя;

x. проверяют подлинность, сервером банковской системы эмитента, многосимвольного PIN зарегистрированного пользователя;

xi. списывают средства, сервером банковской системы эмитента, с финансового счета зарегистрированного пользователя на сумму пополнения, и начисляют сумму пополнения на общий счет при успешной проверке подлинности;

xii. отправляют, сервером банковской системы эмитента, ответ об успешном зачислении денег в механизм аутентификации через электронный коммутатор при успешном начислении на общий счет суммы пополнения;

xiii. обновляют, механизмом аутентификации, счет UPI lite с балансовой стоимостью

на основании суммы пополнения, и создают первую криптограмму ответа авторизации (ARPC) и ответ об успешном обновлении;

xiv. отправляют, механизмом аутентификации, первую ARPC и ответ об успешном обновлении на сервер PSP через электронный коммутатор;

xv. отправляют, сервером PSP, первую ARPC в доверенное приложение через инструмент PSP;

xvi. подтверждают и обновляют, доверенным приложением, балансовую стоимость в безопасной области хранения электронного устройства; и

xvii. отображают, инструментом PSP, обновленную балансовую стоимость зарегистрированному пользователю через интерфейс инструмента PSP.

В одном варианте выполнения этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость для выполнения частично-онлайн транзакции, не затрагивая серверы банковской системы, содержит этапы, на которых:

i. предоставляют возможность, инструментом PSP, зарегистрированному пользователю инициировать платежную транзакцию, при этом платежную транзакцию инициируют зарегистрированным пользователем обеспечением сведений о транзакции, при этом сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции;

ii. запускают, инструментом PSP, доверенное приложение при инициации платежной транзакции чтобы заставить доверенное приложение создавать и возвращать вторую ARQC после выполнения множества заранее определенных проверок, при этом вторая ARQC содержит сведения о транзакции и балансовую стоимость, извлеченные из безопасной области хранения;

iii. отправляют, инструментом PSP, вторую ARQC на сервер PSP;

iv. инициируют, сервером PSP, запрос на платеж в электронный коммутатор при получении второй ARQC;

v. инициируют, электронным коммутатором, запрос на передачу глобального идентификатора на сервер PSP получателя платежа платежной транзакции для получения сведений о финансовом счете получателя платежа;

vi. инициируют, электронным коммутатором, запрос проверки подлинности в механизм аутентификации отправкой второй ARQC в механизм аутентификации;

vii. проверяют подлинность, механизмом аутентификации, ARQC;

viii. списывают средства, механизмом аутентификации, суммы транзакции с балансовой стоимости при успешной проверке подлинности и создают вторую ARPC в

ответ;

ix. отправляют, механизмом аутентификации, созданную вторую ARPC в электронный коммутатор;

x. инициируют, электронным коммутатором, запрос на начисление в сервер банковской системы получателя платежа на основании переданного глобального идентификатора;

xi. отправляют, электронным коммутатором, ответ об успешном начислении вместе со второй ARPC на сервер PSP плательщика при успешном начислении суммы транзакции на счет получателя платежа;

xii. отправляют, сервером PSP, ответ об успешном начислении со второй ARPC в инструмент PSP;

xiii. отправляют, сервером PSP, ответ об успешном начислении и ARPC в доверенное приложение; и

xiv. обновляют, доверенным приложением, балансовую стоимость, хранящуюся в безопасной области хранения на основании ARPC.

В одном варианте выполнения способ дополнительно содержит этап предоставления возможности, инструментом PSP, зарегистрированному пользователю блокировать счет UPI lite, при этом этап содержит следующие подэтапы, на которых:

i. предоставляют возможность, инструментом PSP, зарегистрированному пользователю инициировать блокировку счета UPI lite;

ii. запускают, инструментом PSP, доверенное приложение при инициации блокировки, чтобы заставить доверенное приложение создавать и возвращать третью ARQC после выполнения множества заранее определенных проверок, при этом третья ARQC содержит сведения о финансовом счете зарегистрированного пользователя под получателем платежа, и номер счета lite зарегистрированного пользователя под плательщиком;

iii. отправляют, инструментом PSP, третью ARQC на сервер PSP;

i. инициируют, сервером PSP, запрос на платеж в электронный коммутатор при получении третьей ARQC, при этом запрос на платеж содержит третью ARQC;

ii. пересылают, электронным коммутатором, запрос на платеж в механизм аутентификации;

iii. проверяют подлинность, механизмом аутентификации, полученной ARQC;

iv. списывают средства, механизмом аутентификации, балансовой стоимости при успешной проверке подлинности, и создают третью ARPC в ответ;

v. отправляют, механизмом аутентификации, созданную третью ARPC в

электронный коммутатор;

vi. отправляют, электронным коммутатором, запрос на начисление на сервер банковской системы эмитента для начисления на финансовый счет зарегистрированного пользователя балансовой стоимости;

vii. получают, электронным коммутатором, ответ об успешном начислении с сервера банковской системы эмитента, и пересылают ответ об успешном начислении и третью ARPC на сервер PSP;

viii. отправляют, сервером PSP, ответ об успешном начислении и ARPC в доверенное приложение через инструмент PSP; и

ix. очищают, доверенным приложением, балансовую стоимость, хранящуюся в безопасной области хранения, при получении ARPC.

В одном варианте выполнения этап блокировки счета UPI lite завершается неудачей, когда:

i. на сервере банковской системы эмитента превышено время ожидания;

ii. банковская система эмитента отклонена сервером; и

iii. между сервером PSP и электронным коммутатором происходит потеря сообщения, что затрудняет передачу третьей ARPC и ответ об успешном начислении на сервер PSP.

В одном варианте выполнения этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость для выполнения офлайн транзакции содержит этапы, на которых:

i. предоставляют возможность, инструментом PSP, зарегистрированному пользователю инициировать офлайн платежную транзакцию, при этом офлайн платежную транзакцию инициируют зарегистрированным пользователем установлением канала связи между электронным устройством и устройством получателя платежа для получения сведений о транзакции, при этом сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции;

i. создают, доверенным приложением, офлайн-подпись посредством технологии офлайн аутентификации данных; и

ii. отправляют, доверенным приложением, созданную офлайн-подпись вместе с цифровым сертификатом в инструмент PSP;

iii. отправляют, инструментом PSP, офлайн-подпись в устройство получателя платежа и на сервер PSP;

iv. аутентифицируют, устройством получателя платежа и сервером PSP, инструмент PSP на основании доступной балансовой стоимости в безопасной области хранения,

офлайн-подпись и цифровой сертификат;

v. списывают средства, инструментом PSP, требуемой суммы с балансовой стоимости после успешной аутентификации; и

vi. отправляют, устройством получателя платежа, рекомендацию в механизм аутентификации обновить балансовую стоимость.

В одном варианте выполнения множество заранее определенных проверок содержит одно или несколько из следующего:

- определение того, была ли осуществлена маршрутизация электронного устройства или нет;

- определение того поддерживает ли электронное устройство безопасную область хранения или нет;

- определение того является или нет аттестация ключа достоверной; и

- определение того удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям.

В одном варианте выполнения, параметры транзакции выбирают из группы, состоящей из балансовой стоимости, количества частично-онлайн транзакций, количества офлайн транзакций, суммы транзакции, связанной с частично-онлайн транзакцией, суммы транзакции, связанной с офлайн-транзакцией, общей суммы, связанной с частично-онлайн транзакциями, и общей суммы, связанной с офлайн-транзакциями.

В одном варианте выполнения определение того удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям, содержит определение:

i. является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для частично-онлайн транзакции;

ii. является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для офлайн-транзакции;

iii. является ли сумма транзакции меньшей или равной балансовой стоимости на счете UPI lite;

iv. является ли количество частично-онлайн транзакций меньшим заранее определенного количественного предела онлайн транзакции;

v. является ли количество офлайн-транзакций меньшим заранее определенного количественного предела офлайн-транзакции;

vi. является ли количество офлайн-транзакций меньшим или равным максимальному количеству разрешенных последовательных офлайн транзакций; и

vii. является ли общая сумма офлайн транзакций меньшей или равной заранее

определенному максимальному пределу суммы офлайн-транзакции.

В одном варианте выполнения, первая, вторая и третья ARQC включают одно или несколько из следующего:

a. открытый ключ устройства, хранящийся в безопасной области хранения;

b. блок транзакции, содержащий один или несколько из параметров транзакции, зашифрованных случайным AES ключом, при этом блок транзакции дополнительно зашифрован еще одним AES ключом, который располагается в безопасной области хранения, при этом параметры транзакции содержат одну или несколько единиц следующей информации:

i. сумма транзакции, дата транзакции, время транзакции и глобальный идентификатор получателя платежа;

ii. случайное число;

iii. результат подтверждения клиента;

iv. балансовая стоимость; и

v. счетчик транзакций, степень открытого ключа (асимметричную), тип транзакции и предел баланса.

В одном варианте выполнения доверенное приложение является привязанным к устройству, и определяется на основании параметров, выбираемых из группы, состоящей из идентификатора приложения, идентификатора устройства зарегистрированного пользователя, мобильного номера зарегистрированного пользователя, IFSC сервера банковской системы эмитента и номера финансового счета.

В одном варианте выполнения инструмент PSP выполнен с возможностью обнаруживать случай несанкционированного доступа, и дополнительно выполнен с возможностью вызывать автоматическое и немедленное стирание информации, содержащейся в инструменте PSP, при обнаружении случая несанкционированного доступа.

Настоящее раскрытие дополнительно предусматривает систему для облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн и офлайн платежные транзакции.

КРАТКОЕ ОПИСАНИЕ СОПРОВОЖДАЮЩИХ ЧЕРТЕЖЕЙ

Система и способ облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн и офлайн платежные транзакции настоящего раскрытия теперь будут описаны с помощью сопровождающих чертежей, на которых:

Фигура 1 иллюстрирует блок-схему системы для облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций, в соответствии с настоящим

раскрытием;

Фигура 2 иллюстрирует блок-схему способа облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций, в соответствии с настоящим раскрытием;

Фигура 3 иллюстрирует структурную схему процесса предоставления возможности способа с Фигуры 2, в соответствии с настоящим раскрытием;

Фигура 4A иллюстрирует примерные экраны инструмента PSP, отображающие поток зачисления денег на счет UPI lite, в соответствии с настоящим раскрытием;

Фигура 4B иллюстрирует структурную схему процесса зачисления денег способа с Фигуры 2, в соответствии с настоящим раскрытием;

Фигура 5 иллюстрирует структурную схему предоставления возможности зарегистрированному пользователю выполнять частично-онлайн транзакции способа с Фигуры 2, в соответствии с настоящим раскрытием;

Фигура 6 иллюстрирует структурную схему предоставления возможности зарегистрированному пользователю блокировать счет UPI lite способа с Фигуры 2, в соответствии с настоящим раскрытием; и

Фигура 7 иллюстрирует структурную схему предоставления возможности зарегистрированному пользователю выполнять офлайн транзакции способа с Фигуры 2, в соответствии с настоящим раскрытием.

СПИСОК ССЫЛОЧНЫХ ПОЗИЦИЙ

100 - Система

10 – Электронное устройство/ Мобильное устройство/ Пользовательское устройство

20 – Инструмент поставщика платежной системы (инструмент PSP)

30 – Поставщик платежной системы (PSP)

40 – Сервер банковской системы эмитента / Эмитент CBS/ Отправитель платежа CBS

50 – Сервер банковской системы получателя платежа/ Получатель платежа CBS

102 – Безопасная область хранения (SE/TEE)

104 – Доверенное приложение

106 – Центральный электронный коммутатор

108 – Механизм аутентификации

ПОДРОБНОЕ ОПИСАНИЕ

Варианты выполнения настоящего раскрытия теперь будут описаны со ссылкой на сопровождающие чертежи.

Варианты выполнения обеспечены так, чтобы целиком и полностью передавать

объем настоящего раскрытия специалисту в области техники. Изложены многочисленные сведения, относящиеся к конкретным компонентам, и способы обеспечения полного понимания вариантов выполнения настоящего раскрытия. Специалисту в области техники будет очевидно, что сведения, обеспечиваемые в вариантах выполнения, не должны быть истолкованы как ограничивающие объем настоящего раскрытия. В некоторых вариантах выполнения хорошо известные процессы, хорошо известные структуры устройств и хорошо известные технологии не описаны подробно.

Используемая терминология в настоящем раскрытии, предназначена только для цели объяснения особого варианта выполнения, и такая терминология не должна рассматриваться как ограничивающая объем настоящего раскрытия. Используемые в настоящем раскрытии формы единственного числа могут быть предназначены для того, чтобы включать также формы множественного числа, если контекст явно не предполагает иное. Термины «включающи» и «имеющий» представляют собой неограниченные переходные фразы и, следовательно, указывают на наличие установленных признаков, целых чисел, этапов, операций, элементов и/или компонентов, но не запрещают наличие или добавление одного или нескольких других признаков, целых чисел, этапов, операций, элементов, компонентов и/или их групп. Особый порядок этапов, раскрываемый в способе и процессе настоящего раскрытия, не должен быть истолкован как обязательно требующий их выполнения, как описано или проиллюстрировано. Также следует понимать, что могут быть использованы дополнительные или альтернативные этапы.

Если элемент упоминают как «сцепленный с», «связанный с» или «соединенный с» еще одним элементом, то он может быть непосредственно сцеплен, связан или соединен с другим элементом. Используемый в настоящем документе термин «и/или» включает любой и все совокупности одного или нескольких из связанных перечисленных элементов.

В последние несколько лет, унифицированный платежный интерфейс (UPI) стал одним из приоритетных выборов для клиентов при выполнении розничных платежей. Возможность выполнять платежи посредством смартфонов в 2-3 клика, обеспечила повышенное удобство конечным пользователям. Однако, количество платежных транзакций на основе UPI увеличилось экспоненциально, что привело к увеличению нагрузки по обработке на коммутатор эмитента и серверы банков и поставщиков платежных услуг (PSP). Дополнительно, инфраструктура PSP, способная поддерживать такое большое количество транзакций и обеспечивать надежность с точки зрения показателя успешности, снизилась за несколько последних месяцев.

В дополнение к вышеприведенному, традиционные платежные транзакции на основе мобильных устройств требуют от пользователей обеспечивать конфиденциальную

информацию, такую как UPI PIN, MPIN или пароль для выполнения транзакций на небольшие суммы. Это увеличивает время, необходимое для обработки платежных транзакций на небольшие суммы, что не желательно.

Для того, чтобы решить вышеупомянутые проблемы, настоящее раскрытие предусматривает систему (в дальнейшем называемую «система 100») и способ (в дальнейшем называемый «способ 200») облегчения основанных на правилах частично-онлайн и офлайн платежных транзакций между зарегистрированными пользователями посредством инструментов поставщика платежной системы (PSP).

Со ссылкой на Фигуру 1, система 100 содержит доверенное приложение 104, центральный электронный коммутатор 106 и механизм аутентификации 108. Каждый из зарегистрированных пользователей имеет один или несколько инструментов PSP 20, установленных на их электронных устройствах 10. Каждый из инструментов PSP 20 размещен сервером PSP 30. Зарегистрированные пользователи имеют финансовый счет, связанный с уникальным многосимвольным PIN, и глобальный идентификатор (например, мобильный номер, идентификатор UPI, виртуальный платежный адрес). Инструмент PSP 20 выполнен с возможностью запускать/выполнять доверенное приложение 104 в безопасной области хранения 102 в пределах электронного устройства 10. Безопасная область хранения 102 соответствует элементу безопасности (SE) или доверенной среде выполнения (TEE) электронного устройства 10. Электронный коммутатор 106 соединен с сервером PSP 30, множеством серверов банковской системы (40, 50) и механизмом аутентификации 108. Электронный коммутатор 106 выполнен с возможностью облегчать связь доверенного приложения 104, инструмента PSP 20 и сервера PSP 30 с механизмом аутентификации 108 и множеством серверов банковской системы 40,50, прямо или косвенно, для предоставления возможности зарегистрированному пользователю многочисленных перемещений пользователя: Это включает предоставление возможности зарегистрированному пользователю – регистрировать и создавать счет UPI lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций; зачислять деньги на созданный счет UPI lite с зарегистрированного финансового счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения электронного устройства 10; и использовать балансовую стоимость для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы (40, 50). Перемещения пользователя могут также включать нефинансовые транзакции, такие как справка о балансе и тому подобное.

Соответственно, Фигура 2 иллюстрирует способ 200 облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн

и офлайн платежи. Каждый из зарегистрированных пользователей имеет один или несколько инструментов поставщика платежных услуг (PSP) 20, установленных на их электронных устройствах 10, при этом каждый инструмент PSP 20 размещен сервером PSP 30. Зарегистрированные пользователи имеют финансовый счет, связанный с уникальным многосимвольным PIN и глобальным идентификатором. Способ 200 содержит следующие этапы, на которых:

На этапе 202 инструмент PSP 20, установленный на электронном устройстве 10, связанном с зарегистрированным пользователем, выполняет доверенное приложение 104 в безопасной области хранения электронного устройства 10.

На этапе 204, доверенное приложение 104, инструмент PSP 20 и сервер PSP 30 предоставляют возможность, через центральный электронный коммутатор 106, передавать сообщения с помощью механизма аутентификации 108 и множества серверов банковской системы (40, 50) зарегистрированному пользователю –

- регистрировать и создавать 204a счет lite единого платёжного интерфейса (UPI) для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций;

- зачислять деньги 204b на созданный счет UPI lite с зарегистрированного финансового счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения электронного устройства 10; и

- использовать балансовую стоимость 204c для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы (40, 50), при этом балансовая стоимость подобна токену или цифровому активу, и имеет информацию о стоимости актива, владельце актива, эмитенте и дереве Меркла последних нескольких транзакций.

Система 100 облегчает зарегистрированному пользователю регистрироваться с помощью механизма аутентификации 108 и создавать счет UPI lite. Счет UPI lite предоставляет возможность зарегистрированному пользователю выполнять частично-онлайн и офлайн платежные транзакции на небольшую сумму, с другими зарегистрированными пользователями и платежными агентами. Инструмент PSP 20, используемый зарегистрированными пользователями, может уже иметь один или несколько счетов, добавленных для предоставления возможности зарегистрированным пользователям выполнять онлайн платежные транзакции. Термин «зарегистрированные пользователи», используемый в настоящем документе, относится к пользователям, которым уже предоставлен доступ к серверу UPI/ механизму аутентификации 108 для выполнения (полностью) онлайн платежных транзакций на основе UPI. На основе конфигурации связанных эмитентов, сервер PSP 30, на котором размещен инструмент PSP

20, может также напоминать пользователям настроить UPI счет для выполнения частично-онлайн и офлайн транзакций.

Например, если зарегистрированный пользователь зарегистрирован в нескольких банках (A, B, C) для выполнения полностью онлайн транзакций на основе UPI, а банк «A» поддерживает создание счета UPI lite, то сервер PSP 30 может отображать возможность «Предоставлена возможность UPI счета» ниже названия банка «A» на экране дисплея устройства 10 через интерфейс инструмента PSP. При нажатии «Предоставлена возможность UPI счета», инструмент PSP отправляет запрос на вызов открытого ключа в доверенное приложение 104. В ответ, доверенное приложение 104 создает пару персональный (Ps) - открытый (Pk) ключ непосредственно внутри безопасной области хранения 102, подобно TEE электронного устройства 10. Созданный открытый ключ отправляют в механизм аутентификации 108 инструментом PSP 20 через сервер PSP 30 и электронный коммутатор 106. Механизм аутентификации 108 подписывает открытый ключ (Pk) вместе с некоторыми другими сведениями, такими как идентификатор устройства, номер счета, мобильный номер, глобальный идентификатор и т.д., для создания цифрового сертификата (DC-Pk) (также называемого «стандартный сертификат транзакции/STC»). Механизм аутентификации 108 создает уникальный номер счета UPI lite и открывает соответствующий счет UPI lite для зарегистрированного пользователя. Этот цифровой сертификат (DC-Pk) снабжен механизмом аутентификации 108, а также доверенным приложением 104 для аутентификации будущих транзакций с этого устройства 10.

В одном варианте выполнения, ссылаясь на Фигуру 3, этап предоставления возможности зарегистрированному пользователю регистрировать и создавать 204a счет UPI lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций содержит этапы, на которых:

На этапе получения 302 инструмент PSP 20 получает команду предоставления возможности услуги от зарегистрированного пользователя через интерфейс инструмента PSP, при этом команда предоставления возможности услуги содержит сведения о финансовом счете, к которому должна быть предоставлена возможность выполнения частично-онлайн и офлайн транзакций. Другими словами, зарегистрированному пользователю предоставляют возможность выбирать финансовый счет, к которому должна быть предоставлена возможность, из одного или нескольких ранее существующих финансовых счетов, через интерфейс инструмента PSP, выполнять платежные частично-онлайн и офлайн платежные транзакции.

На этапе 204 инструмент PSP создает запрос на вызов открытого ключа при получении команды предоставления возможности услуги, и отправляет запрос на вызов

созданного открытого ключа в доверенное приложение 104.

На этапе 306 доверенное приложение 104 создает пару персональный (Ps) - открытый (Pk) ключ в пределах безопасной области хранения электронного устройства 10 при получении запроса на вызов открытого ключа от инструмента PSP.

На этапе 308 доверенное приложение 104 отправляет открытый ключ (Ps) из созданной пары персональный-открытый ключ (Ps-Pk) в инструмент PSP 20.

На этапе 310 инструмент PSP 20 создает запрос о списке ключей при получении открытого ключа, при этом запрос о списке ключей содержит созданный открытый ключ (Pk).

На этапе 312 инструмент PSP 20 передает созданный запрос о списке ключей в электронный коммутатор 106 через сервер PSP 30, связанный с инструментом PSP 20.

На этапе 314 электронный коммутатор 106 осуществляет маршрутизацию запроса о списке ключей, полученного с сервера PSP 30, в механизм аутентификации 108.

На этапе 316 механизм аутентификации 108 открывает счет UPI lite для зарегистрированного пользователя созданием цифрового сертификата (DC-Pk) посредством открытого ключа и обновляют запрос предоставления возможности услуг с помощью номера уникального счета lite, при этом запрос предоставления возможности услуги указывает на открытие счета UPI lite для зарегистрированного пользователя, а уникальный номер счета lite представляет собой уникальный номер счета, связанный со счетом UPI lite. Цифровой сертификат содержит открытый ключ, встроенный в него, с дополнительной информацией, описывающей владельца, т.е., зарегистрированного пользователя, связанного с открытым ключом. Дополнительная информация может включать, но не ограничиваться этим, имя, почтовый адрес, идентификатор устройства, номер счета, мобильный номер, глобальный идентификатор и адрес электронной почты зарегистрированного пользователя. Цифровой сертификат (Pk) и открытый ключ снабжены механизмом аутентификации 108 и доверенным приложением 104 для аутентификации будущих частично-онлайн или офлайн транзакций, инициируемых с электронного устройства 10. Цифровой сертификат (Pk) и открытый ключ могут быть сохранены в компании или в отдельном хранилище, или в облачном сервере.

На этапе 318 механизм аутентификации 108 создает успешный ответ о списке ключей при успешном открытии счета UPI lite и сохранении открытого ключа.

На этапе 320 механизм аутентификации 108 передает сообщение с успешным ответом о списке ключей в инструмент PSP 20 через электронный коммутатор 106 и сервер PSP 30 для уведомления зарегистрированного пользователя об успешном предоставлении возможности услуги для соответствующего финансового счета.

Примерные псевдокоды, отображающие функции инструмента PSP 20, доверенного приложения 104 и механизма аутентификации 108 следующие –

Инструмент PSP –

Читать (команда предоставления возможности услуги);

Делать

{

Создавать запрос на вызов открытого ключа;

Отправлять запрос на вызов открытого ключа в доверенное приложение;

Делать

{

Создавать запрос о списке ключей;

Передавать созданный запрос о списке ключей в механизм аутентификации через сервер PSP и электронный коммутатор;

}

в то же время (считывая открытый ключ из доверенного приложения)

}

Доверенное приложение или общая библиотека –

Делать

{

Создавать пару персональный (Ps) – открытый (Pk) ключ в пределах безопасной области хранения;

Отправлять открытый ключ в инструмент PSP;

}

В то же время (считывая запрос на вызов открытого ключа)

Механизм аутентификации –

Делать

{

получать запрос о списке ключей;

открывать счет UPI lite для зарегистрированного пользователя созданием цифрового сертификата (DC-Pk) посредством открытого ключа в пределах запроса о списке ключей;

обновлять запрос предоставления возможности услуг с уникальным номером счета lite;

создавать успешный ответ о списке ключей;

отправлять успешный ответ о списке ключей в инструмент PSP 20 через электронный коммутатор и сервер PSP для уведомления зарегистрированного пользователя

об успешном предоставлении возможности услуги для соответствующего финансового счета.

}

Этап предоставления возможности зарегистрированному пользователю регистрировать и создавать счет UPI lite для выполнения основанных на правилах платежных транзакции завершается неудачей, когда происходит потеря сообщения между сервером PSP 30 и электронным коммутатором 106.

Зарегистрированный пользователь может передавать деньги на счет UPI lite в любой момент времени с помощью инструмента PSP 20. При транзакции зачисления денег, зарегистрированному пользователю необходимо ввести многосимвольный PIN, как показано на Фигуре 4A. Деньги могут быть зачислены на счет UPI lite только из финансового счета (финансовых счетов), выбранного для предоставления возможности во время процесса регистрации.

Механизм аутентификации 108 выполнен с возможностью хранить список зарегистрированных пользователей (т.е. имена пользователей или уникальные идентификационные номера, связанные со счетами пользователя), и балансовую стоимость, заранее определенные параметры, открытый ключ и цифровой сертификат, связанный с каждым из зарегистрированных пользователей. При получении запроса на зачисление денег от зарегистрированного пользователя, механизм аутентификации 108 обновляет балансовую стоимость, связанную с зарегистрированным пользователем, после того, как многосимвольный PIN зарегистрированного пользователя успешно прошел проверку подлинности сервером банковской системы эмитента 40.

В одном варианте выполнения, ссылаясь на Фигуру 4B, этап предоставления возможности зарегистрированному пользователю зачислять деньги 204b на созданный счет UPI lite с зарегистрированного финансового счета, содержит этапы, на которых:

На этапе 402 инструмент PSP 20 создает напоминание о вводе PIN и суммы в интерфейсе инструмента PSP для извлечения многосимвольного PIN, и суммы пополнения от зарегистрированного пользователя для зачисления суммы на созданный счет UPI lite. Инструмент PSP 20 получает многосимвольный PIN и сумму пополнения через интерфейс инструмента PSP. Сумму пополнения и многосимвольный PIN отправляют в доверенное приложение 104. При получении суммы пополнения и многосимвольного PIN, доверенное приложение 104 напоминает зарегистрированному пользователю выполнить подтверждение первого уровня. Подтверждение первого уровня может быть выполнено, например, введением предварительно установленного PIN или пароля блокировки устройства, введением предварительно установленного шаблона экрана блокировки, или

реализацией сканирования устройством отпечатка пальца.

На этапе 404 доверенное приложение 104 выполняет множество заранее определенных проверок. Заранее определенные проверки включают, но не ограничиваются этим, определение того была ли осуществлена маршрутизация электронного устройства или нет, определение того, поддерживает ли электронное устройство безопасную область хранения или нет, определение того, является или нет аттестация ключа достоверной, и определение того, удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям. Например, параметр транзакции может быть текущей балансовой стоимостью, максимально допустимой балансовой стоимостью или минимальной стоимостью для пополнения денежных средств. Соответственно, заранее определенным критерием может быть то, была ли сумма пополнения плюс балансовая стоимость меньшей или равной максимально допустимой балансовой стоимости. Альтернативно, заранее определенным критерием может быть то, является ли сумма пополнения большей минимальной стоимости для пополнения денежных средств. В одном примере, если максимально допустимая балансовая стоимость составляет 2000 рупий, то доверенное приложение 104 проверяет то, является ли сумма пополнения, когда она добавлена к балансовой стоимости, меньшей или равной 2000 рупий. При успешной проверке доверенное приложение 104 создает первый блок учетных данных, содержащий многосимвольный PIN, и второй блок учетных данных, содержащий первую криптограмму запроса авторизации (ARQC). Инструмент PSP 20 получает созданный первый и второй блоки учетных данных от доверенного приложения 104. Первая ARQC содержит сведения о транзакции и результаты проверки параметров, зашифрованные случайным AES ключом, при этом AES ключ зашифрован персональным ключом (Ps). Сведения о транзакции содержат глобальный идентификатор зарегистрированного пользователя в качестве сведений о плательщике, номер счета UPI lite в качестве сведений о получателе платежа, сумму пополнения в качестве суммы транзакции, дату транзакции и время транзакции.

На этапе 406 инструмент PSP 20 инициирует запрос на зачисление денег на сервер PSP 30. Запрос на зачисление денег содержит первый и второй блоки учетных данных.

На этапе 408 сервер PSP 30 отправляет запрос на зачисление денег в механизм аутентификации 108 через электронный коммутатор 106.

На этапе 410 механизм аутентификации 108 проверяет подлинность запроса предоставления возможности услуги первой ARQC при получении запроса на зачисление денег. Проверка подлинности включает проверку подлинности первой ARQC посредством цифрового сертификата, соответствующего зарегистрированному пользователю. Это

включает расшифровку первой ARQC посредством открытого ключа и сопоставление расшифрованного блока (содержащего AES зашифрованные сведения о транзакции и результаты проверки параметров) со сведениями, хранящимися в механизме аутентификации 108.

На этапе 412 электронный коммутатор 106 пересылает запрос на зачисление денег на сервер банковской системы эмитента 40, связанный с финансовым счетом зарегистрированного пользователя.

На этапе 414 сервер банковской системы эмитента 40 проверяет подлинность многосимвольного PIN зарегистрированного пользователя.

На этапе 414 сервер банковской системы эмитента 40 списывает средства с финансового счета зарегистрированного пользователя на сумму пополнения и начисляет сумму пополнения на общий счет при успешной проверке подлинности. Таким образом, чтобы предоставить возможность платежных транзакций на основе UPI lite, денежные средства размещают в пределах сервера банковской системы 40. Другими словами, при получении запроса на зачисление денег и успешной аутентификации PIN зарегистрированного пользователя, сервер банковской системы передает денежные средства со счета зарегистрированного пользователя на общий счет/виртуальный счет, принадлежащий банку.

На этапе 416 сервер банковской системы эмитента 40 отправляет ответ об успешном зачислении денег в механизм аутентификации 108 через электронный коммутатор 106, при успешном начислении на общий счет суммы пополнения.

На этапе 418 механизм аутентификации 108 обновляет счет UPI lite балансовой стоимостью на основании суммы пополнения, и создает первую криптограмму ответа авторизации (ARPC) и ответ об успешном обновлении.

На этапе 420 механизм аутентификации 108 отправляет первую ARPC и ответ об успешном обновлении на сервер PSP 30 через электронный коммутатор 106.

На этапе 422 сервер PSP 30 отправляет первую ARPC в доверенное приложение 104 через инструмент PSP 20.

На этапе 424 доверенное приложение 104 подтверждает получение первой ARPC и обновляет балансовую стоимость в безопасной области хранения электронного устройства 10, чтобы балансовая стоимость в безопасной области хранения совпадала с балансовой стоимостью на счете UPI lite механизма аутентификации 108. Таким образом, как только сервер банковской системы эмитента 40 подтверждает успешную передачу денежных средств на общий счет, предоставляется возможность услуги UPI lite, и балансовая стоимость отражается в доверенном приложении.

На этапе 426 инструмент PSP 20 отображает обновленную балансовую стоимость зарегистрированному пользователю через интерфейс инструмента PSP.

Примерные псевдокоды инструмента PSP 20, доверенного приложения, механизма аутентификации 108 и сервера банковской системы эмитента 40 следующие –

Инструмент PSP –

Считывать (многосимвольный PIN и сумму пополнения);

Делать

{

Отправлять полученную сумму пополнения и многосимвольный PIN в доверенное приложение;

Получать первый и второй блок учетных данных от доверенного приложения;

Создавать и отправлять запрос на зачисление денег в механизм аутентификации;

Получать первую ARPC с сервера PSP и отправлять полученную первую ARPC в доверенное приложение;

}

Доверенное приложение или общая библиотека –

Делать

{

Получать сумму пополнения и многосимвольный PIN;

выполнять подтверждение первого уровня зарегистрированного пользователя;

выполнять множество заранее определенных проверок и создавать соответствующие результаты;

Если (результаты == удовлетворительные)

{

создавать первый блок учетных данных, содержащий многосимвольный PIN; создавать второй блок учетных данных, содержащий первую криптограмму запроса авторизации (ARQC);

отправлять созданные блоки учетных данных в инструмент PSP;

}

Получать первую ARPC из инструмента PSP;

Подтверждать получение первой ARPC;

Обновлять балансовую стоимость в безопасной области хранения электронного устройства, чтобы она соответствовала балансовой стоимости на счете UPI lite механизма аутентификации;

}

Сервер банковской системы эмитента –

Делать

{

Получать запрос на зачисление денег через электронный коммутатор;

Проверять подлинность многосимвольного PIN зарегистрированного пользователя;

Если (статус проверки подлинности == успех)

{

списывать средства с финансового счета зарегистрированного пользователя на сумму пополнения, и начислять сумму пополнения на общий счет при успешной проверке подлинности;

если (списание средств и начисление == успешные)

{

отправлять ответ об успешном зачислении денег в механизм аутентификации;

}

}

}

Механизм аутентификации –

Делать

{

Получать запрос на зачисление денег;

Проверять подлинность первой ARQC;

Получать статус зачисления денег;

Если (статус зачисления денег == успех)

{

обновлять счет UPI lite балансовой стоимостью на основании суммы пополнения;

создавать первую криптограмму ответа авторизации (ARPC) и ответ об успешном обновлении;

отправлять первую ARPC в инструмент PSP через сервер PSP и электронный коммутатор;

}

}

Транзакция зачисления денег завершается неудачей, когда сервер банковской системы эмитента 40 отклоняет транзакцию из-за отказа списания средств со счета зарегистрированного пользователя или отказа начисления на общий счет. В этом случае сервер банковской системы эмитента 40 может быть выполнен с возможностью отправлять

соответствующий код ответа в электронный коммутатор 106. Электронный коммутатор 106 может инициировать запрос в механизм аутентификации 108 и вызов первой ARPC. Электронный коммутатор 106 может затем пересылать то же самое на сервер PSP 30. Сервер PSP 30 пересылает то же самое в инструмент PSP 20 для обновления доверенного приложения 104.

Транзакция зачисления денег может дополнительно завершаться неудачей, когда превышено время ожидания списания средств на сервере банковской системы эмитента 40. В этом случае электронный коммутатор 106 инициирует запрос в механизм аутентификации 108 для первой ARPC. Электронный коммутатор 106 пересылает первую ARPC в конечный ответ на сервер PSP 30. Сервер PSP 30 отправляет то же самое в инструмент PSP 20 для обновления доверенного приложения 104. Соответственно, транзакции рассчитывают в операционном отделе банка.

Транзакция зачисления денег дополнительно завершается неудачей, когда между сервером PSP 30 и электронным коммутатором 106 происходит потеря сообщения, что затрудняет передачу первой ARPC и ответ об успешном обновлении на сервер PSP 30. В этом случае, сервер PSP 30 инициирует синхронизацию между доверенным приложением 104 и механизмом аутентификации 108.

Доверенное приложение 104 хранит балансовую стоимость и заранее определенные критерии в безопасной области хранения 102 для облегчения транзакций с низким ордером. Балансовую стоимость поддерживают на уровне доверенного приложения, а сервер банковской системы эмитента 40 ответственен за пополнение балансовой стоимости. Балансовую стоимость зашифровывают посредством персонального ключа шифрования, созданного в пределах безопасной области хранения 102 доверенным приложением 104. Зарегистрированные пользователи могут использовать, посредством этой балансовой стоимости, создание платежей в течение доли секунды, не требуя никакого PIN, и использованием PIN только для разблокирования мобильного устройства/ инструмента PSP. Это уменьшит нагрузку на серверы эмитента 40 и электронный коммутатор 106, и поможет зарегистрированным пользователям выполнять транзакции на небольшие суммы, не раскрывая онлайн PIN и баланс, доступный в центральной банковской системе.

Механизм аутентификации 108 облегчает синхронизацию между балансовой стоимостью в безопасной области хранения 102 электронного устройства 10, и балансовой стоимостью в механизме аутентификации 108 в любое время.

В одном варианте выполнения ссылаясь на Фигуру 5, этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость 204c для выполнения частично-онлайн транзакции, не затрагивая серверы банковской

системы (40, 50), содержит следующие этапы, на которых:

На этапе 502 инструмент PSP 20 предоставляет возможность зарегистрированному пользователю инициировать платежную транзакцию, при этом платежную транзакцию инициируют зарегистрированным пользователем обеспечением сведений о транзакции. Сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции. Транзакция может быть инициирована сканированием статического QR и введением суммы транзакции, сканированием динамического QR-кода, который включает сумму транзакции, ручным вводом глобального адреса/VPA получателя платежа и суммы транзакции в интерфейсе инструмента PSP, или получением глобального идентификатора получателя платежа и сведений о сумме транзакции через NFC с терминала платежного агента.

На этапе 504 инструмент PSP 20 запускает доверенное приложение 104 при инициации платежной транзакции. Это заставляет доверенное приложение 104 создавать и возвращать, на этапе 506, вторую ARQC после выполнения множества заранее определенных проверок, при этом вторая ARQC содержит сведения о транзакции и балансовой стоимости, извлеченные из безопасной области хранения электронного устройства. Во второй ARQC, сведения о транзакции и балансовой стоимости могут быть зашифрованы с помощью случайного AES ключа, при этом AES ключ зашифрован персональным ключом (Ps). Информация о транзакции содержит глобальный идентификатор получателя платежа, глобальный идентификатор плательщика/зарегистрированного пользователя, сумму транзакции и результаты множества заранее определенных проверок. Например, заранее определенные проверки, выполняемые доверенным приложением 104, включают проверку того, подходит ли транзакция для частично-онлайн транзакции сравнением суммы транзакции с балансовой стоимостью, хранящейся в безопасной области хранения 102, и/или сравнением суммы транзакции с максимально допустимой суммой транзакции для частично-онлайн транзакции. Транзакция подходит для частично-онлайн транзакции, если сумма транзакции меньше балансовой стоимости, хранящейся в безопасной области хранения 102, и дополнительно сумма транзакции меньше максимально допустимой суммы транзакции.

На этапе 508 инструмент PSP 20 отправляет вторую ARQC на сервер PSP 30.

На этапе 510 сервер PSP 30 инициирует запрос на платеж в электронный коммутатор 106 при получении второй ARQC.

На этапе 512 электронный коммутатор 106 инициирует запрос на передачу глобального идентификатора на сервер PSP 60 получателя платежа платежной транзакции для получения сведений о финансовом счете получателя платежа. Сервер PSP 60

получателя платежа идентифицируют из глобального идентификатора получателя платежа.

На этапе 514 электронный коммутатор 106 инициирует запрос проверки подлинности в механизм аутентификации 108 отправкой второй ARQC в механизм аутентификации 108.

На этапе 516 механизм аутентификации 108 проверяет подлинность второй ARQC. Проверка подлинности включает проверку подлинности второй ARQC посредством цифрового сертификата, соответствующего зарегистрированному пользователю. Это включает расшифровку ARQC посредством предварительно сохраненного открытого ключа (Pk), соответствующего зарегистрированному пользователю, и сопоставление расшифрованного блока (содержащего AES зашифрованную информацию о транзакции и результаты проверки параметров) со сведениями, хранящимися в механизме аутентификации 108.

На этапе 518 механизм аутентификации 108 списывает средства суммы транзакции с балансовой стоимости при успешной проверке подлинности, и создает вторую ARPC в ответ.

На этапе 520 механизм аутентификации 108 отправляет созданную вторую ARPC в электронный коммутатор 106.

На этапе 522 электронный коммутатор 106 инициирует запрос на начисление в сервер банковской системы получателя платежа 50 на основании переданного глобального идентификатора.

На этапе 524 электронный коммутатор 106 отправляет ответ об успешном начислении вместе со второй ARPC на сервер PSP плательщика 30 при успешном начислении суммы транзакции на счет получателя платежа.

На этапе 526 сервер PSP 30 оправляет ответ об успешном начислении со второй ARPC в инструмент PSP 20.

На этапе 528 сервер PSP 30 отправляет ответ об успешном начислении и ARPC в доверенное приложение 104.

На этапе 530 доверенное приложение 104 обновляет балансовую стоимость, хранящуюся в безопасной области хранения, на основании ARPC.

Примерные псевдокоды, отображающие функции инструмента PSP 20, доверенного приложения 104, электронного коммутатора 106 и механизма аутентификации 108 следующие –

Инструмент PSP –

Делать

{

Получать сведения о транзакции от зарегистрированного пользователя;

Запускать доверенное приложение для создания и возвращения второй ARQC;

Инструмент PSP отправляет вторую ARQC в электронный коммутатор через сервер PSP;

}

Электронный коммутатор –

Делать

{

Получать вторую ARQC;

Инициировать запрос на передачу глобального идентификатора на сервер PSP получателя платежа для получения сведений о финансовом счете получателя платежа;

Инициировать запрос проверки подлинности в механизм аутентификации отправкой ему второй ARQC;

Если (вторая ARPC получена == да)

{

Инициировать запрос на начисление в сервер банковской системы получателя платежа;

Если (начисление успешно == да)

{

отправлять ответ об успешном начислении вместе со второй ARPC в инструмент PSP через сервер PSP плательщика;

}

}

}

Доверенное приложение или общая библиотека –

Делать

{

Получать запуск из инструмента PSP для создания и возвращения второй ARQC;

Выполнять множество заранее определенных проверок;

Если (результаты проверок == удовлетворительные)

{

Создавать и возвращать вторую ARQC;

}

Получать ответ об успешном начислении и вторую ARPC из инструмента PSP;

Обновлять балансовую стоимость в безопасной области хранения на основании

второй ARPC;

}

Механизм аутентификации –

Делать

{

Проверять подлинность второй ARQC;

Списывать средства суммы транзакции с балансовой стоимости;

Если (списание средств == успешное)

{

Создавать вторую ARPC в ответ.

Отправлять созданную вторую ARPC в электронный коммутатор;

}

Балансовая стоимость, доступная в безопасной области хранения 102, будет первой точкой принятия решения для доверенного приложения 104, чтобы решить выполнять или нет частично-онлайн транзакцию.

В случае, если балансовая стоимость не обновляется из-за сетевого подключения, она будет обновляться, когда электронное устройство 10 будет онлайн или, когда произойдет последующая транзакция. Механизм аутентификации 108 решает должна ли транзакция быть полностью онлайн или частично-онлайн транзакцией на основании доступной балансовой стоимости. Полностью онлайн транзакция может быть выполнена традиционным образом извлечением PIN от пользователя и выполнением проверки подлинности PIN на сервере 40 эмитента.

В итоге, частично-онлайн транзакции инициируют зарегистрированными пользователями сканированием статического/динамического QR-кода или прикосновением электронного устройства 10 к терминалу платежного агента для выполнения сканирования и оплаты/транзакции на основе NFC для использования балансовой стоимости при покупке товаров. Частично-онлайн транзакция представляет собой транзакцию, которую выполняют посредством балансовой стоимости, и утверждают эмитентом прокси, т.е. механизмом аутентификации 108, на основе сохраненной балансовой стоимости и требуемых критериев аутентификации.

В одном варианте выполнения частично-онлайн транзакция завершается неудачей, когда –

а) запрос на начисление отклоняют сервером банковской системы получателя платежа: в этом случае, электронный коммутатор 106 может инициировать отмену списания средств в механизме аутентификации 108. Новая вторая ARPC может быть

создана механизмом аутентификации 108 и отправлена на сервер PSP 30. Сервер PSP 30 может облегчать обновление доверенного приложения 104 при отказе транзакции.

b) сервер банковской системы получателя платежа считает транзакцию совершенной.

c) между сервером PSP 30 и электронным коммутатором 106 происходит потеря сообщения, что затрудняет передачу ответа об успешном начислении вместе со второй ARPC на сервер PSP: в этом случае сервер PSP 30 может инициировать синхронизацию с электронным коммутатором 106, электронный коммутатор 106 может вызывать вторую ARPC с последним обновлением статуса в механизме аутентификации 108, и сервер PSP 30 может использовать эту ARPC для обновления доверенного приложения 104 окончательным статусом.

d) серверу PSP 30 зарегистрированного пользователя не удается отправить ответ об успешном начислении со второй ARPC в инструмент PSP 20: В этом случае, сервер PSP 30 может повторять попытки до тех пор, пока вторая ARPC не будет успешно передана в инструмент PSP 20; в случае, когда серверу PSP 30 не удается сохранить вторую ARPC, сервер PSP 30 может вызвать инструмент PSP 20 для инициирования синхронизации, чтобы снова вызвать вторую ARPC из электронного коммутатора 106.

e) инструменту PSP 20 не удается отправить ответ об успешном начислении со второй ARPC в доверенное приложение: В этом случае, инструмент PSP 20 повторяет попытки до тех пор, пока доверенное приложение 104 не будет обновлено.

В одном варианте выполнения этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость 204c для выполнения офлайн транзакции, содержит следующие этапы, на которых. Сначала инструмент PSP 20 предоставляет возможность зарегистрированному пользователю инициировать офлайн платежную транзакцию, при этом офлайн платежную транзакцию инициируют зарегистрированным пользователем установлением канала связи между электронным устройством 10 и устройством получателя платежа для получения сведений о транзакции. Сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции. После этого доверенное приложение 104 создает офлайн-подпись посредством технологии офлайн-аутентификации данных (ODA). Технология ODA, используемая в настоящем документе, может быть стандартной технологией офлайн-аутентификации. Офлайн-подпись может быть создана на основе строки динамических данных, содержащей параметры, такие как сумма транзакции, идентификатор транзакции, отметка времени транзакции, номер плательщика счета lite, глобальный адрес получателя платежа, мобильный номер плательщика/зарегистрированного пользователя и

идентификатор устройства. Доверенное приложение 104 отправляет созданную офлайн-подпись и предварительно сохраняет цифровой сертификат в инструменте PSP 20. Инструмент PSP 20 отправляет офлайн-подпись на устройство получателя платежа и сервер PSP 30. Устройство получателя платежа и сервер PSP 30 аутентифицируют инструмент PSP 20 на основании доступной балансовой стоимости в безопасной области хранения 102, офлайн-подписи и цифрового сертификата. Инструмент PSP 20 списывает средства требуемой суммы с балансовой стоимости после успешной аутентификации. Устройство получателя платежа отправляет рекомендацию в механизм аутентификации 108 обновить балансовую стоимость.

В примерном варианте выполнения, ссылаясь на Фигуру 7, для выполнения офлайн транзакции, зарегистрированный пользователь открывает инструмент PSP 20 на своем электронном устройстве 10 и выбирает возможность «Коснуться и Оплатить». С «Коснуться и Оплатить» на экране, зарегистрированный пользователь касается электронным устройством 10 терминала платежного агента для инициирования транзакции. Таким образом, транзакцию инициируют посредством канала NFC между электронным устройством 10 и терминалом платежного агента. На основе доступной балансовой стоимости в безопасной области хранения 102 и взаимоподдерживаемого способа офлайн-аутентификации данных (ODA), терминал платежного агента аутентифицирует инструмент PSP 20 и запрашивает одобрение транзакции. Терминал и инструмент PSP 20 определяют, какой способ ODA поддерживается, после чего терминал запрашивает инструмент PSP 20 для создания цифровой подписи посредством поддерживаемого способа ODA. В зависимости от используемого способа, ODA может гарантировать, что инструмент PSP 20 и доверенное приложение 104 являются подлинными, и что ключевая информация о транзакции не была изменена во время передачи. После успешной аутентификации, инструмент PSP 20 списывает требуемую сумму с балансовой стоимости и одобряет транзакцию. Стандартный способ подтверждения устройства может быть использован для подтверждения зарегистрированного пользователя. После успешной транзакции терминал отправляет рекомендацию в механизм аутентификации 108 обновить балансовую стоимость и заранее определенные параметры.

Во время офлайн-транзакции, могут быть два сценария отказа –

- проблема с электронным устройством 10 во время транзакции – В этом случае, сумма транзакции не будет вычтена из балансовой стоимости зарегистрированного пользователя.

- проблема с электронным устройством 10 после завершения транзакции – Если какая-либо сторона выходит онлайн, балансовая стоимость проверяется на подлинность и

реализуется после обработки транзакции, и впоследствии зарегистрированный пользователь сможет использовать это для будущих транзакций. Пока не будет выполнена онлайн синхронизация с механизмом аутентификации 108, балансовая стоимость не может использоваться ни для каких транзакций.

В одном варианте выполнения инструмент PSP 20 обеспечивает возможность для зарегистрированного пользователя отказаться от счета UPI. При подтверждении, выполняют подтверждение устройства в один клик механизмом аутентификации 108, и осуществляют отказ от регистрации деактивацией счета UPI lite пользователя и удалением открытых-персональных ключей.

Ссылаясь на Фигуру 6, способ 200 содержит этап предоставления возможности инструментом PSP 20, зарегистрированному пользователю блокировать счет UPI lite. Этап содержит следующие подэтапы, на которых –

На этапе 602 инструмент PSP 20 предоставляет возможность зарегистрированному пользователю инициировать блокировку счета UPI lite.

На этапе 604 инструмент PSP 20 запускает доверенное приложение 104 при инициации блокировки. Это заставляет доверенное приложение 104, на этапе 606, создавать и возвращать третью ARQC после выполнения множества заранее определенных проверок. Третья ARQC содержит сведения о финансовом счете зарегистрированного пользователя под получателем платежа, и номер счета lite зарегистрированного пользователя под плательщиком.

На этапе 608 инструмент PSP 20 отправляет третью ARQC на сервер PSP 30.

На этапе 610 сервер PSP 30 инициирует запрос на платеж в электронный коммутатор 106 при получении третьей ARQC. Запрос на платеж содержит третью ARQC.

На этапе 612 электронный коммутатор 106 пересылает запрос на платеж в механизм аутентификации 108.

На этапе 614 механизм аутентификации 108 проверяет подлинность полученной третьей ARQC и списывает средства балансовой стоимости при успешной проверке подлинности, и создает третью ARPC в ответ.

На этапе 616 механизм аутентификации 108 отправляет созданную третью ARPC в электронный коммутатор 106.

На этапе 618 электронный коммутатор 106 отправляет запрос на начисление на сервер банковской системы эмитента 40 для начисления на финансовый счет зарегистрированного пользователя балансовой стоимости.

На этапе 620 электронный коммутатор 106 получает ответ об успешном начислении с сервера банковской системы эмитента 40 и пересылает ответ об успешном начислении и

третью ARPC на сервер PSP 30.

На этапе 622 сервер PSP 30 отправляет ответ об успешном начислении и третью ARPC в доверенное приложение 104 через инструмент PSP 20.

На этапе 624 доверенное приложение 104 очищает балансовую стоимость, хранящуюся в безопасной области хранения при получении третьей ARPC.

В одном варианте выполнения этап блокировки счета UPI lite завершается неудачей, когда – (i) превышено время ожидания на сервере банковской системы эмитента 40, (ii) банковская система эмитента 40 отклонена сервером, и/или (iii) происходит потеря сообщения между сервером PSP 30 и электронным коммутатором 106, что затрудняет передачу третьей ARPC и ответ об успешном начислении на сервер PSP 30.

Инструмент PSP 20 облегчает зарегистрированному пользователю извлечение счета UPI lite, не требуя многосимвольного PIN от пользователя. Если инструмент PSP 20 не знает есть ли у зарегистрированного пользователя счет UPI lite, он может предоставить возможность зарегистрированному пользователю добавить финансовый счет. Однако в этом случае, зарегистрированному пользователю могут напомнить ввести PIN для подтверждения на сервере банковской системы эмитента 40.

В дополнительном варианте выполнения инструмент PSP 20 предоставляет возможность зарегистрированному пользователю проверять баланс, связанный со счетом UPI lite. Транзакция справки о балансе будет самозапускаемой транзакцией, в которой механизм аутентификации 108 будет синхронизировать свой баланс со значением баланса, хранящимся в безопасной области хранения 102 электронного устройства 10. В этой транзакции доверенное приложение 104 будет создавать криптограмму запроса авторизации (ARQC) с нулем в качестве входных данных для тех элементов, которые относятся к транзакции покупки.

Доверенное приложение 104 поддерживает обнаружение многослойного несанкционированного доступа и механизмы ответа. Доверенное приложение 104 внедряет механизмы управления доступом, чтобы гарантировать то, что данные доверенного приложения 104 не доступны еще одному мобильному приложению. Доверенное приложение 104 также может обеспечивать канал, который поддерживает и защищает передачу сообщений с внешними системами.

Доверенное приложение 104 может быть выполнено за одно целое с одним или несколькими сторонними приложениями в качестве SDK, и поддерживает интеграцию на основе API для доставки обновлений в бизнес-процессы. Оно имеет безопасный механизм обновления, чтобы позволять осуществлять подтверждение целостности программного обеспечения приложений, когда их загружают в ядро.

Доверенное приложение 104 становится доступным только для тех пользователей, электронные устройства 10 которых поддерживают безопасную область хранения 102. Безопасную область хранения 102 реализуют либо в программном обеспечении, либо в аппаратуре, либо в совокупности программного обеспечения и аппаратуры (например, элемент безопасности или TEE). Возможные реализации таких решений включают:

- Использование трастлета, запускающегося в доверенной среде выполнения для шифрования и управления всеми требующими безопасности конфиденциальными данными, и/или размещения платежного ядра;

- Использование апплета, запускающегося в элементе безопасности, основанном на аппаратуре, для шифрования и управления всеми требующими безопасности конфиденциальными данными, и/или размещения платежного ядра; и

- Использование совокупности способности конкретной аппаратуры устройства, такой как хранилище ключей Android, для реализации безопасного хранения и способов программного обеспечения для шифрования и управления всеми требующими безопасности конфиденциальными данными.

Безопасная область хранения 102 может иметь две функции: (i) поддерживать безопасность выполнения криптографического алгоритма, не открывая ключевой материал, и (ii) гарантировать то, что конфиденциальные данные остаются в зашифрованном виде при хранении в телефонном аппарате.

Множество заранее определенных проверок, раскрываемых в настоящем документе, содержат одно или несколько из следующих:

- определение того, была ли осуществлена маршрутизация электронного устройства или нет;

- определение того поддерживает ли электронное устройство безопасную область хранения или нет;

- определение того является или нет аттестация ключа достоверной;

- определение того удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям.

Параметры транзакции выбирают из группы, состоящей из балансовой стоимости, количества частично-онлайн транзакций, количества офлайн транзакций, суммы транзакции, связанной с частично-онлайн транзакцией, суммы транзакции, связанной с офлайн-транзакцией, общей суммы, связанной с частично-онлайн транзакциями, и общей суммы, связанной с офлайн-транзакциями. Дополнительно, определение того удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям, содержит определение:

- является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для частично-онлайн транзакции;

- является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для офлайн-транзакции;

- является ли сумма транзакции меньшей или равной балансовой стоимости на счете UPI lite;

- является ли количество частично-онлайн транзакций меньшим заранее определенного количественного предела онлайн транзакции;

- является ли количество офлайн-транзакций меньшим заранее определенного количественного предела офлайн-транзакции;

- является ли количество офлайн-транзакций меньшим или равным максимальному количеству разрешенных последовательных офлайн транзакций; и

- является ли общая сумма офлайн транзакций меньшей или равной заранее определенному максимальному пределу суммы офлайн-транзакции.

Первая, вторая и третья ARQC, раскрытые в настоящем документе, включают одно или несколько из следующего:

- открытый ключ устройства 10, хранящийся в безопасной области хранения 102;

- блок транзакции, содержащий один или несколько из параметров транзакции, зашифрованных случайным AES ключом, при этом блок транзакции дополнительно зашифрован персональным ключом, который располагается в безопасной области хранения, при этом параметры транзакции содержат, но не ограничиваются этим, одну или несколько единиц следующей информации:

- сведения о транзакции, содержащие сумму транзакции или сумму пополнения, дату транзакции, время транзакции, и глобальный идентификатор получателя платежа, и номер счета UPI lite;

- случайное число;

- результат подтверждения клиента;

- балансовая стоимость; и

- счетчик транзакций, степень открытого ключа (асимметричную), тип транзакции и предел баланса.

Доверенное приложение 104 является привязанным к устройству и определяется на основе параметров, выбираемых из группы, состоящей из идентификатора приложения, идентификатора устройства зарегистрированного пользователя, мобильного номера зарегистрированного пользователя, IFSC сервера банковской системы эмитента 40 и номера финансового счета.

Дополнительно, когда меняют устройство, сервер PSP 30 инициирует запрос о списке ключей с новым значением идентификатора устройства. Записи, сохраненные механизмом аутентификации 108 для зарегистрированного пользователя, будут обновлены. В случае, когда зарегистрированный пользователь удаляет инструмент PSP 20 и серверу PSP 30 необходимо извлекать сведения об услуге lite, сервер PSP 30 активирует запрос о списке ключей для вызова номера услуги lite/уникального номера счета lite, после чего следует вызов синхронизации для статуса lite.

Предпочтительно, инструмент PSP 20 выполнен с возможностью обнаруживать случай несанкционированного доступа, и дополнительно выполнен с возможностью вызывать автоматическое и немедленное стирание информации, содержащейся в инструменте PSP 20, при обнаружении случая несанкционированного доступа.

В одном варианте выполнения, если механизм аутентификации 108 обнаруживает, что зарегистрированный пользователь вовлечен в потенциальное мошенничество или, если подлинный клиент вызывает эмитента и сообщает об утере своего электронного устройства 10, механизм аутентификации 108 добавляет запись сертификата зарегистрированного пользователя в список аннулированных сертификатов (CRL). Также, механизм аутентификации 108 воздерживается от выпуска нового сертификата устройства для пользователя в случае, когда они обнаружены в этом списке.

В случае, когда зарегистрированный пользователь удаляет инструмент PSP 20 или идентификатор (ID) устройства меняется, и при регистрации того же самого зарегистрированного пользователя на том же самом устройстве или еще одном устройстве, будет предусмотрен возврат баланса. Инструмент PSP 20 будет запускать запрос о регистрации на основе заранее определенного целевого кода. Система 100 проверяет услуги UPI lite на соответствие мобильному номеру в данном инструменте PSP 20. Если имеется баланс, связанный с услугой lite. Информация, относящаяся к транзакции возврата, будет отправлена на сервер банковской системы эмитента 40.

Как и исходные онлайн UPI транзакции, UPI lite также взаимозаменяемы, что означает, что зарегистрированный пользователь может передавать денежные средства посредством счета UPI lite на любой банковский счет.

Во избежание главного риска множественных офлайн транзакций, механизм аутентификации 108 может быть выполнен с возможностью связываться с терминалами платежного агента для облегчения терминалам платежного агента поддерживать список отказов. Список отказов может быть периодически обновлен в соответствии со списком аннулированных сертификатов (CRL), опубликованным механизмом аутентификации 108. Таким образом, система 100 допускает зарегистрированным пользователям выполнять

только заранее определенное количество офлайн транзакций.

Предпочтительно, сервер PSP 30 выполнен с возможностью обеспечивать уникальный идентификационный номер для каждого из номеров счетов каждого из зарегистрированных пользователей. Сервер PSP 30 гарантирует, что для одного и того же финансового счета зарегистрированного пользователя, уникальный идентификационный номер всегда будет тем же самым.

Предпочтительно, доверенное приложение 104 содержит модуль удаления. Инструмент PSP 20 выполнен с возможностью запускать модуль выхода из системы, когда намерение о выходе из системы получено от зарегистрированного пользователя. При получении намерения о выходе из системы, модуль выхода из системы выполнен с возможностью удалять персональный ключ из безопасной области хранения 102 электронного устройства 10.

Предпочтительно, все транзакции UPI lite проверяют на подлинность механизмом аутентификации 108 посредством проверки подлинности криптограммы (ARPC/ARQC). Доверенное приложение 104 выполнено с возможностью запрещать обработку транзакций через счет UPI lite, если он не получает ARPC (криптограмму ответа) из механизма аутентификации 108. Если ARPC не получена доверенным приложением 104 для транзакции, где создана ARQC, инструмент PSP 20 временно остановит/задержит все транзакции UPI lite до получения ARPC из механизма UPI lite. Сервер PSP 30 будет инициировать синхронизацию с механизмом аутентификации 108 для получения обновленной ARPC, что позволит доверенному приложению 104 синхронизироваться с механизмом аутентификации 108. Дополнительно, если превышено время ожидания до аутентификации транзакции механизмом аутентификации 108, инструмент PSP 20 будет иметь возможность синхронизировать баланс с механизмом аутентификации 108, и восстанавливать баланс для транзакции, которая была инициирована.

В случае превышения времени ожидания, инструмент PSP 20 может быть выполнен с возможностью инициировать запрос на проверку транзакции для синхронизации с механизмом аутентификации 108. ARPC будет содержать последний обновленный статус механизма аутентификации 108 и это предоставит возможность доверенному приложению 104 синхронизироваться с механизмом аутентификации 108. Если механизм аутентификации 108 не способен обеспечивать обновление синхронизации в инструмент PSP 20, услуги lite будут временно заблокированы до выполнения успешной синхронизации. Успешная синхронизация подразумевает, что механизм аутентификации 108 обеспечил удостоверенную ARPC в инструмент PSP 20, и доверенное приложение 104 подтвердило то же самое.

Чтобы предоставлять возможность серверам банковской системы (40, 50) выполнять согласование для транзакции UPI lite, механизм аутентификации 108 может быть выполнен с возможностью обеспечивать файл, содержащий подробные данные о транзакции lite на сервер банковской системы эмитента 40 и о балансовой стоимости во время создания взаиморасчета. Сервер банковской системы 40 будет списывать денежные средства с соответствующего общего/виртуального счета пользователя услуги lite. Впоследствии, сервер банковской системы 40 будет сопоставлять балансовую стоимость зарегистрированного пользователя (после списания средств с общего/виртуального счета) с балансовой стоимостью, обеспечиваемой механизмом аутентификации 108. Если баланс совпадает, то согласование является успешным.

В одном примерном варианте выполнения, для облегчения частично-онлайн и офлайн транзакций, инструмент PSP 20 может быть выполнен с возможностью выполнять множественные проверки, такие как – проверка подлинности из доверенного приложения 104, доступна ли сумма транзакции для обработки транзакции, проверка подлинности на основании суммы, вводимой пользователем, если сумма подходит для транзакций lite, инициирование синхронизации в случае, когда ARPC не получена для какой-либо транзакции lite, в которой ARQC была инициирована, в случае если ответ на запрос синхронизации не получен, после заранее определенного периода времени и заранее определенного количества попыток синхронизации, обработка транзакций через полностью онлайн-поток транзакций (с двухфакторной аутентификацией), предложение зарегистрированному пользователю уведомления пополнить баланс в случае, если балансовая стоимость ниже заранее определенной суммы (например, 200 рупий), гарантирование того, что сумма пополнения не превышает заранее установленную сумму (например, 2000 рупий) на основе балансовой стоимости, доступной в безопасной области хранения 102, получение согласия клиента (на предоставление услуг lite перед инициацией потока предоставления возможности, и инициирование автоматической блокирки услуги lite, если зарегистрированный пользователь не выполнил никаких финансовых транзакций в течение заранее определенного периода времени (в случае, если пользователь отказался от устройства/закрытия счета).

Аналогично, доверенное приложение 104 может быть выполнено с возможностью сохранять проверку ARPC, полученную с предыдущей транзакции. Если то же самое не было получено, то доверенное приложение 104 не будет инициировать ARQC для последующих транзакций.

Для замены аутентификации на основе PIN и уменьшения зависимости от серверов центрального банка эмитента, настоящее раскрытие обеспечивает форму аутентификации,

которая эффективно использует инфраструктуру открытого ключа (PKI) и безопасное хранилище с поддержкой аппаратуры на устройствах потребителей, подходящих для транзакций с низкой стоимостью. Секретный ключ (Ps) или персональный ключ, уникальный для банковского счета пользователя, безопасно хранят на устройстве 10, и он служит для строгой аутентификации транзакций с низкой стоимостью. Безопасный ключ хранят в криптографическом хранилище с поддержкой аппаратуры (HbCV) (элемент безопасности или TEE или хранилище ключей «Strongbox», при наличии) на подтвержденном устройстве 10 потребителя. Поскольку требование о подтверждении PIN удаляют для транзакций на небольшие суммы, отказы транзакций из-за технологического отклонение (TD) и спада бизнеса (BD), например, из-за недействительного многосимвольного PIN и недостаточности денежных средств, резко уменьшаются. Это улучшает общий показатель успешности транзакций на небольшие суммы. В частности, в каждом случае зарегистрированный пользователь добавляет денежные средства в размере 2000 рупий на счет UPI lite, приблизительно 28-33 операции менее 200 рупий предотвращают в инфраструктуре банковской системы. Технологические отклонения для UPI lite, связанные с финансовыми транзакциями, удаляют, поскольку предотвращают переход на сервер банковской системы эмитента. Благодаря этому показатели успешности повышаются примерно на 5%.

Настоящее раскрытие дополнительно предусматривает настраиваемое решение балансовой стоимости, которое дополняет любой тип цифровой платежной услуги независимо от способа взаиморасчета, например, мгновенную оплату на основе QR или запасную стоимость с замкнутым циклом и т.д. Балансовая стоимость может быть задействована несколькими методами, например, предварительной авторизацией, дополнительными запасными стоимостями для эмитентов или кредитов. Транзакция может быть передана посредством любого типа бесконтактного взаимодействия, например, динамического QR, NFC, Bluetooth или Sound, а платежный агент может подтверждать платеж с помощью мобильного приложения, ПК или любого устройства. Доверенное приложение 104 настоящего изобретения поддерживает технологии обработки интеллектуальных правил синхронно с электронным коммутатором 106, а также технологии подтверждения состояния одного или нескольких приложений на мобильном устройстве 10, пытающихся выполнять неожиданные функции доверенной среды выполнения, а также перемещение состояния приложения из доверенной среды выполнения с первого мобильного устройства 10 на второе мобильное устройство 10 в случае, когда мобильное устройство 10 взломано, утеряно, украдено, повреждено или обновляется.

Функции, описываемые в настоящем документе, могут быть реализованы в аппаратуре, программном обеспечении, выполняемом процессором, встроенным программным обеспечением или любой их совокупностью. При реализации в программном обеспечении, выполняемом процессором, функции могут быть сохранены или переданы в виде одной или нескольких инструкций, или кода на машиночитаемом носителе. Другие примеры и реализации находятся в пределах объема и сути раскрытия и приложенной формулы изобретения. Например, за счет сути программного обеспечения, функции, описываемые выше, могут быть реализованы посредством программного обеспечения, выполняемого процессором, аппаратуры, встроенного программного обеспечения, проводной схемы или совокупности любых из них. Признаки реализующих функций могут также быть физически расположены в различных положениях, в том числе распределяться так, чтобы части функций были реализованы в различных физических положениях.

Вышеизложенное описание вариантов выполнения было обеспечено с целью иллюстрации и не предназначено для ограничения объема настоящего раскрытия. Отдельные компоненты особого варианта выполнения в общем не ограничены этим особым вариантом выполнения, а являются взаимозаменяемыми. Такие вариации не должны рассматриваться как отступление от настоящего раскрытия, а все такие модификации считают находящимися в пределах объема настоящего раскрытия.

ТЕХНОЛОГИЧЕСКИЙ ПРОГРЕСС

Настоящее раскрытие, описываемое в настоящем документе выше, имеет несколько технологических преимуществ, включающих, но не ограничиваясь ими, реализацию системы и способа, которые:

- облегчают основанные на правилах частично-онлайн и офлайн платежные транзакции;

- облегчают платежные транзакции, не требуя от пользователей раскрывать конфиденциальную информацию, такую как PIN или пароль;

- это уменьшает нагрузку по обработке платежей на коммутатор эмитента, поставщиков платежных услуг и на банковские серверы;

- облегчают основанные на правилах транзакции на небольшие суммы, не затрагивая банковские серверы;

- облегчают платежные транзакции, подлежащие выполнению, безопасным образом;

- помогают в масштабировании обработки транзакции с минимальными затратами на инфраструктуру;

- гарантируют взаиморасчет денежных средств систематическим образом;

- уменьшают отказы транзакций из-за технологического отклонения (TD) и спада

бизнеса (BD), например, из-за недействительного многосимвольного PIN и недостаточности денежных средств, и улучшают общий показатель успешности транзакций на небольшие суммы; и

- предоставляют возможность зарегистрированным пользователям выполнять платежные транзакции в один клик.

Варианты выполнения настоящего документа и различные их признаки и предпочтительные сведения объясняют со ссылкой на неограничивающие варианты выполнения в следующем описании. Описания хорошо известных компонентов и технологий обработки опущены, чтобы излишне не осложнять варианты выполнения настоящего документа. Примеры, используемые в настоящем документе, предназначены просто для облегчения понимания методов, в которых варианты выполнения настоящего документа могут быть осуществлены, и для дополнительного предоставления возможности специалистам в области техники осуществлять варианты выполнения настоящего документа. Соответственно, примеры не должны быть истолкованы как ограничивающие объем вариантов выполнения настоящего документа.

Вышеизложенное описание конкретных вариантов выполнения настолько полно раскрывает общую суть вариантов выполнения настоящего документа, что другие могут, применением современных знаний, легко модифицировать и/или адаптировать для различных применений, таких как конкретные варианты выполнения без отступления от оригинального замысла, а, следовательно, такие адаптации и модификации должны и предназначены для того, чтобы быть понятными в пределах значения и диапазона эквивалентов раскрытых вариантов выполнения. Должно быть понято, что фразеология или терминология, используемые в настоящем документе, предназначены для описания, а не для ограничения. Следовательно, хотя варианты выполнения настоящего документа были описаны с точки зрения предпочтительных вариантов выполнения, специалисты в области техники признают, что варианты выполнения настоящего документа могут быть осуществлены с модификацией в пределах сути и объема вариантов выполнения, описываемых в настоящем документе.

Использование выражения «по меньшей мере» или «по меньшей мере один» предлагает использование одного или нескольких элементов, или ингредиентов или количеств, поскольку использование может быть в варианте выполнения раскрытия для достижения одной или нескольких из описываемых задач или результатов.

Хотя в настоящем документе значительное внимание было уделено компонентам и частям компонентов предпочтительных вариантов выполнения, следует понимать, что могут быть выполнены многие варианты выполнения, и что многие изменения могут быть

выполнены в предпочтительных вариантах выполнения без отступления от принципов раскрытия. Эти и другие изменения в предпочтительном варианте выполнения, а также в других вариантах выполнения будут очевидны специалистам в области техники из раскрытия настоящего документа, при этом должно быть отчетливо понятно, что вышеизложенный текстовый материал должен быть интерпретирован просто в качестве иллюстративного раскрытия, а не ограничения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ (200) облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн и офлайн платежные транзакции, при этом каждый из зарегистрированных пользователей имеет один или несколько инструментов (20) поставщиков платежных услуг (PSP), установленных на их электронных устройствах (10), при этом каждый инструмент PSP (20) размещен сервером PSP (30), при этом зарегистрированные пользователи имеют финансовый счет, связанный с уникальным многосимвольным PIN и глобальным идентификатором, при этом указанный способ (200) включает этапы, на которых:

- выполняют (202), посредством инструмента PSP (20), установленного на электронном устройстве (10), связанном с зарегистрированным пользователем, доверенное приложение (104) в безопасной области хранения электронного устройства (10).

- предоставляют возможность (204), через центральный электронный коммутатор (106), доверенное приложение (104), инструмент PSP (20) и сервер PSP (30) осуществлять связь с механизмом аутентификации (108) и множеством серверов банковской системы (40, 50) для предоставления возможности зарегистрированному пользователю:

- регистрировать и создавать (204a) единый платежный интерфейс счета (UPI) lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций;

- зачислять деньги (204b) на созданный счет UPI lite с зарегистрированного финансового счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения; и

- использовать балансовую стоимость (204c) для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы (40, 50).

2. Способ (200) по п. 1, в котором этап предоставления возможности зарегистрированному пользователю регистрировать и создавать (204a) счет UPI lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций, содержит этапы, на которых:

i. получают (302), посредством инструмента PSP (20), команду предоставления возможности услуги от зарегистрированного пользователя через интерфейс инструмента PSP, при этом команда предоставления возможности услуги содержит сведения о финансовом счете, к которому предоставляется возможность выполнения частично-онлайн и офлайн транзакций;

ii. создают (304), посредством инструмента PSP (20), запрос на вызов открытого

ключа при получении команды предоставления возможности услуги, и отправляют запрос на вызов созданного открытого ключа доверенному приложению (104);

iii. создают (306), доверенным приложением (104), пару персональный (Ps) - открытый (Pk) ключ в пределах безопасной области хранения электронного устройства (10) при получении запроса на вызов открытого ключа от инструмента PSP (20);

iv. отправляют (308), доверенным приложением (104), открытый ключ из созданной пары персональный-открытый ключ в инструмент PSP (20);

v. создают (310), посредством инструмента PSP (20), запрос о списке ключей при получении открытого ключа, при этом запрос о списке ключей содержит открытый ключ;

vi. передают (312), посредством инструмента PSP (20), созданный запрос о списке ключей в электронный коммутатор (106) через сервер PSP (30), связанный с инструментом PSP (20);

vii. осуществляют маршрутизацию (314), электронным коммутатором (106), запроса о списке ключей, полученного с сервера PSP (30), в механизм аутентификации (108);

viii. открывают (316) посредством механизма аутентификации (108), счет UPI lite для зарегистрированного пользователя созданием цифрового сертификата (DC-Pk) посредством открытого ключа и обновляют запрос предоставления возможности услуги с помощью уникального номера счета lite, при этом цифровой сертификат (Pk) и открытый ключ снабжены механизмом аутентификации (108) для аутентификации будущих частично-онлайн или офлайн транзакций, инициируемых с электронного устройства (10);

ix. создают (318) посредством механизма аутентификации (108), успешный ответ о списке ключей при успешном открытии счета UPI lite и сохраняют открытый ключ; и

x. передают (320) посредством механизма аутентификации (108), успешный ответ о списке ключей в инструмент PSP (20) через электронный коммутатор (106) и сервер PSP (30) для уведомления зарегистрированного пользователя об успешном предоставлении возможности услуги для соответствующего финансового счета.

3. Способ (200) по п. 1, в котором этап предоставления возможности зарегистрированному пользователю зачислять деньги (204b) на созданный счет UPI lite с зарегистрированного финансового счета содержит этапы, на которых:

i. создают (402), посредством инструмента PSP (20), напоминание о вводе PIN и суммы в интерфейсе инструмента PSP, для извлечения многосимвольного PIN и суммы пополнения от зарегистрированного пользователя для зачисления суммы на созданный счет UPI lite;

ii. получают (402), посредством инструмента PSP, многосимвольный PIN и сумму

пополнения через интерфейс инструмента PSP;

iii. напоминают (402), доверенным приложением (104), зарегистрированному пользователю выполнить подтверждение первого уровня посредством сканирования устройством отпечатка пальца;

iv. создают (404), доверенным приложением (104), первый блок учетных данных, содержащий многосимвольный PIN, и второй блок учетных данных, содержащий первую криптограмму запроса авторизации (ARQC), после выполнения множества заранее определенных проверок;

v. получают (404), посредством инструмента PSP (20), созданный первый и второй блок учетных данных от доверенного приложения (104);

vi. инициируют (406), посредством инструмента PSP (20), запрос на зачисление денег в сервер PSP (30), при этом запрос на зачисление денег содержит первый и второй блок учетных данных;

vii. отправляют (408), посредством сервера PSP (30), запрос на зачисление денег в механизм аутентификации (108) через электронный коммутатор (106);

viii. проверяют подлинность (410), посредством механизма аутентификации (108), запроса сервиса предоставления возможности услуги первой ARQC, при получении запроса на зачисление денег;

ix. пересылают (412), посредством электронного коммутатора (106), запрос на зачисление денег на сервер банковской системы (40) эмитента, связанный с финансовым счетом зарегистрированного пользователя;

x. проверяют подлинность (414), посредством сервера банковской системы эмитента (40), многосимвольного PIN зарегистрированного пользователя;

xi. списывают средства (414), посредством сервера банковской системы эмитента (40), с финансового счета зарегистрированного пользователя на сумму пополнения, и начисляют сумму пополнения на общий счет при успешной проверке подлинности;

xii. отправляют (416), посредством сервера банковской системы эмитента (40) ответ об успешном зачислении денег в механизм аутентификации (108) через электронный коммутатор (106) при успешном начислении на общий счет суммы пополнения;

xiii. обновляют (418), посредством механизма аутентификации (108), счет UPI lite с балансовой стоимостью на основании суммы пополнения, и создают первую криптограмму ответа авторизации (ARPC) и ответ об успешном обновлении;

xiv. отправляют (420), посредством механизма аутентификации (108), первую ARPC и ответ об успешном обновлении на сервер PSP (30) через электронный коммутатор (106);

xv. отправляют (422), посредством сервера PSP (30) первую ARPC в доверенное приложение (104) через инструмент PSP (20);

xvi. подтверждают и обновляют (424), доверенным приложением (104), балансовую стоимость в безопасной области хранения электронного устройства (10); и

xvii. отображают (426), посредством инструмента PSP (20), обновленную балансовую стоимость зарегистрированному пользователю через интерфейс инструмента PSP.

4. Способ (200) по п. 1, в котором этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость (204c) для выполнения частично-онлайн транзакции, не затрагивая серверы банковской системы (40, 50), содержит этапы, на которых:

i. предоставляют возможность (502), посредством инструмента PSP (20), зарегистрированному пользователю инициировать платежную транзакцию, при этом платежную транзакцию инициируют зарегистрированным пользователем обеспечением сведений о транзакции, при этом сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции;

ii. запускают (504), посредством инструмента PSP (20), доверенное приложение (104) при инициации платежной транзакции, чтобы заставить доверенное приложение (104) создавать и возвращать (506) вторую ARQC после выполнения множества заранее определенных проверок, при этом вторая ARQC содержит сведения о транзакции и балансовой стоимости, извлеченные из безопасной области хранения;

iii. отправляют (508), посредством инструмента PSP (20), вторую ARQC на сервер PSP (30);

iv. инициируют (510), посредством сервера PSP (30), запрос на платеж в электронный коммутатор (106) при получении второй ARQC;

v. инициируют (512), посредством электронного коммутатора (106), запрос на передачу глобального идентификатора на сервер PSP получателя платежа (60) платежной транзакции для получения сведений о финансовом счете получателя платежа;

vi. инициируют (514), посредством электронного коммутатора (106), запрос проверки подлинности в механизм аутентификации (108) отправкой второй ARQC в механизм аутентификации (108);

vii. проверяют подлинность (516), посредством механизма аутентификации (108), второй ARQC;

viii. списывают средства (518), посредством механизма аутентификации (108),

суммы транзакции с балансовой стоимости при успешной проверке подлинности, и создают вторую ARPC в ответ;

ix. отправляют (520), посредством механизма аутентификации (108), созданную вторую ARPC в электронный коммутатор (106);

x. инициируют (522), посредством электронного коммутатора (106), запрос на начисление в сервер банковской системы получателя платежа (50) на основании переданного глобального идентификатора;

xi. отправляют (524), посредством электронного коммутатора (106), ответ об успешном начислении вместе со второй ARPC на сервер PSP плательщика (30) при успешном начислении суммы транзакции на счет получателя платежа;

xii. отправляют (526), посредством сервера PSP (30), ответ об успешном начислении со второй ARPC в инструмент PSP (20);

xiii. отправляют (528), посредством сервера PSP (30), ответ об успешном начислении и ARPC в доверенное приложение (104); и

xiv. обновляют (530), доверенным приложением (104), балансовую стоимость, хранящуюся в безопасной области хранения, на основании ARPC.

5. Способ (200) по п. 1, который дополнительно содержит этап предоставления возможности, посредством инструмента PSP (20), зарегистрированному пользователю блокировать счет UPI lite, при этом указанный этап содержит следующие подэтапы, на которых:

i. предоставляют возможность (602), посредством инструмента PSP, зарегистрированному пользователю инициировать блокировку счета UPI lite;

ii. запускают (604), посредством инструмента PSP (20), доверенное приложение (104) при инициации блокировки, чтобы заставить доверенное приложение (104) создавать и возвращать (606) третью ARQC после выполнения множества заранее определенных проверок, при этом третья ARQC содержит сведения о финансовом счете зарегистрированного пользователя под получателем платежа, и номер счета lite зарегистрированного пользователя под плательщиком;

iii. отправляют (608), посредством инструмента PSP (20), третью ARQC на сервер PSP (30);

iv. инициируют (610), посредством сервера PSP (30), запрос на платеж в электронный коммутатор (106) при получении третьей ARQC, при этом запрос на платеж содержит третью ARQC;

v. пересылают (612), посредством электронного коммутатора (106), запрос на

платеж в механизм аутентификации (108);

vi. проверяют подлинность (614), посредством механизма аутентификации (108), полученной ARQC;

vii. списывают средства (614), посредством механизма аутентификации (108), балансовой стоимости при успешной проверке подлинности, и создают третью ARPC в ответ;

viii. отправляют (616), посредством механизма аутентификации (108), созданную третью ARPC в электронный коммутатор (106);

ix. отправляют (618), посредством электронного коммутатора (106) запрос на начисление на сервер банковской системы эмитента (40) для начисления на финансовый счет зарегистрированного пользователя балансовой стоимости;

x. получают (620), посредством электронного коммутатора (106), ответ об успешном начислении с сервера банковской системы эмитента (40) и пересылают ответ об успешном начислении и третью ARPC на сервер PSP (30);

xi. отправляют (622), посредством сервера PSP (30), ответ об успешном начислении и ARPC в доверенное приложение (104) через инструмент PSP (20); и

xii. очищают (624), доверенным приложением (104), балансовую стоимость, хранящуюся в безопасной области хранения, при получении ARPC.

6. Способ (200) по п. 3, в котором этап зачисления денег на созданный счете UPI lite с зарегистрированного финансового счета завершается неудачей, когда:

i. сервер банковской системы эмитента (40) отклоняет транзакцию из-за отказа списания средств со счета зарегистрированного пользователя или отказа начисления на общий счет;

ii. превышено время ожидания списания средств на сервере банковской системы эмитента (40); и

iii. между сервером PSP (30) и электронным коммутатором (106) происходит потеря сообщения, что затрудняет передачу первой ARPC и ответ об успешном обновлении на сервер PSP (30).

7. Способ (200) по п. 5, в котором этап блокировки счета UPI lite завершается неудачей, когда:

i. превышено время ожидания на сервере банковской системы эмитента (40);

ii. банковская система эмитента (40) отклонена сервером; и

iii. между сервером PSP (30) и электронным коммутатором (106) происходит потеря сообщения, что затрудняет передачу третьей ARPC и ответ об успешном начислении на

сервер PSP (30).

8. Способ (200) по п. 4, в котором частично-онлайн транзакция завершается неудачей, когда:

i. запрос на начисление отклоняют сервером банковской системы (50) получателя платежа;

ii. сервер банковской системы получателя платежа (50) считает транзакцию совершенной;

iii. между сервером PSP (30) и электронным коммутатором (106) происходит потеря сообщения, что затрудняет передачу ответа об успешном начислении вместе со второй ARPC на сервер PSP (30);

iv. серверу PSP (30) зарегистрированного пользователя не удается отправить ответ об успешном начислении со второй ARPC в инструмент PSP (20); и

v. инструменту PSP (20) не удается отправить ответ об успешном начислении со второй ARPC в доверенное приложение (104).

9. Способ (200) по п. 1, в котором этап предоставления возможности зарегистрированному пользователю использовать балансовую стоимость (204c) для выполнения офлайн транзакции, содержит этапы, на которых:

i. предоставляют возможность, посредством инструмента PSP (20), зарегистрированному пользователю инициировать офлайн платежную транзакцию, при этом офлайн платежную транзакцию инициируют зарегистрированным пользователем установлением канала связи между электронным устройством (10) и устройством получателя платежа для получения сведений о транзакции, при этом сведения о транзакции включают глобальный идентификатор получателя платежа и сумму транзакции;

ii. создают, доверенным приложением (104), офлайн-подпись посредством технологии офлайн аутентификации данных (ODA); и

iii. отправляют, доверенным приложением (104), созданную офлайн-подпись вместе с цифровым сертификатом в инструмент PSP (20);

iv. отправляют, посредством инструмента PSP (20), офлайн-подпись и цифровой сертификат на устройство получателя платежа;

v. аутентифицируют, устройством получателя платежа, инструмент PSP (20) на основании доступной балансовой стоимости в безопасной области хранения (102), офлайн-подпись и цифровой сертификат;

vi. списывают средства, посредством инструмента PSP (20), требуемой суммы с балансовой стоимости после успешной аутентификации; и

vii. отправляют, устройством получателя платежа, рекомендацию в механизм аутентификации (108) обновить балансовую стоимость.

10. Способ (200) по п.п. 1, 2 и 3, в котором множество заранее определенных проверок содержит одно или несколько из следующего:

i. определение того, была ли осуществлена маршрутизация электронного устройства или нет;

ii. определение того, поддерживает ли электронное устройство безопасную область хранения или нет;

iii. определение того, является или нет аттестация ключа достоверной; и

iv. определение того, удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям.

11. Способ (200) по п. 10, в котором параметры транзакции выбирают из группы, состоящей из балансовой стоимости, количества частично-онлайн транзакций, количества офлайн транзакций, суммы транзакции, связанной с частично-онлайн транзакцией, суммы транзакции, связанной с офлайн-транзакцией, общей суммы, связанной с частично-онлайн транзакциями, и общей суммы, связанной с офлайн-транзакциями.

12. Способ (200) по п. 10, в котором определение того, удовлетворяет или нет один или несколько параметров транзакции одному или нескольким заранее определенным критериям, содержит определение:

i. является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для частично-онлайн транзакции;

ii. является ли сумма транзакции меньшей или равной максимальному значению суммы транзакции для офлайн-транзакции;

iii. является ли сумма транзакции меньшей или равной балансовой стоимости на счете UPI lite;

iv. является ли количество частично-онлайн транзакций меньшим заранее определенного количественного предела онлайн транзакции;

v. является ли количество офлайн-транзакций меньшим заранее определенного количественного предела офлайн-транзакции;

vi. является ли количество офлайн-транзакций меньшим или равным максимальному количеству разрешенных последовательных офлайн транзакций; и

vii. является ли общая сумма офлайн транзакций меньшей или равной заранее определенному максимальному пределу суммы офлайн-транзакции.

13. Способ (200) по п.п. 1, 2 и 3, в котором первая, вторая и третья ARQC содержат

одно или несколько из следующего:

i. открытый ключ устройства, хранящийся в безопасной области хранения (102);

ii. блок транзакции, содержащий один или несколько из параметров транзакции, зашифрованных случайным AES ключом, при этом блок транзакции дополнительно зашифрован еще одним AES ключом, который располагается в безопасной области хранения, при этом параметры транзакции содержат одну или несколько единиц следующей информации:

- сведения о транзакции, содержащие сумму транзакции или сумму пополнения, дату транзакции, время транзакции и глобальный идентификатор получателя платежа, и номер счета UPI lite;

- случайное число;

- результат подтверждения клиента;

- балансовая стоимость; и

- счетчик транзакций, степень открытого ключа (асимметричную), тип транзакции и предел баланса.

14. Способ (200) по п. 1, в котором доверенное приложение является привязанным к устройству и определяется на основе параметров, выбранных из группы, состоящей из идентификатора приложения, идентификатора устройства зарегистрированного пользователя, мобильного номера зарегистрированного пользователя, IFSC сервера банковской системы эмитента (40) и номера финансового счета.

15. Способ (200) по п. 1, в котором инструмент PSP (20) обнаруживает случай несанкционированного доступа, и дополнительно вызывает автоматическое и немедленное стирание информации, содержащейся в инструменте PSP (20), при обнаружении случая несанкционированного доступа.

16. Система (100) облегчения зарегистрированным пользователям выполнять основанные на правилах частично-онлайн и офлайн платежные транзакции, при этом каждый из зарегистрированных пользователей имеет один или несколько инструментов (20) поставщиков платежных услуг (PSP), установленных на их электронных устройствах (10), при этом каждый инструмент PSP (20) размещен сервером PSP (30), зарегистрированные пользователи имеют финансовый счет, связанный с уникальным многосимвольным PIN и глобальным идентификатором, при этом указанная система (100) включает:

- выполняемое доверенное приложение (104), инструментом PSP (20), установленное на электронном устройстве (10), связанном с зарегистрированным

пользователем, в безопасной области хранения электронного устройства (10);

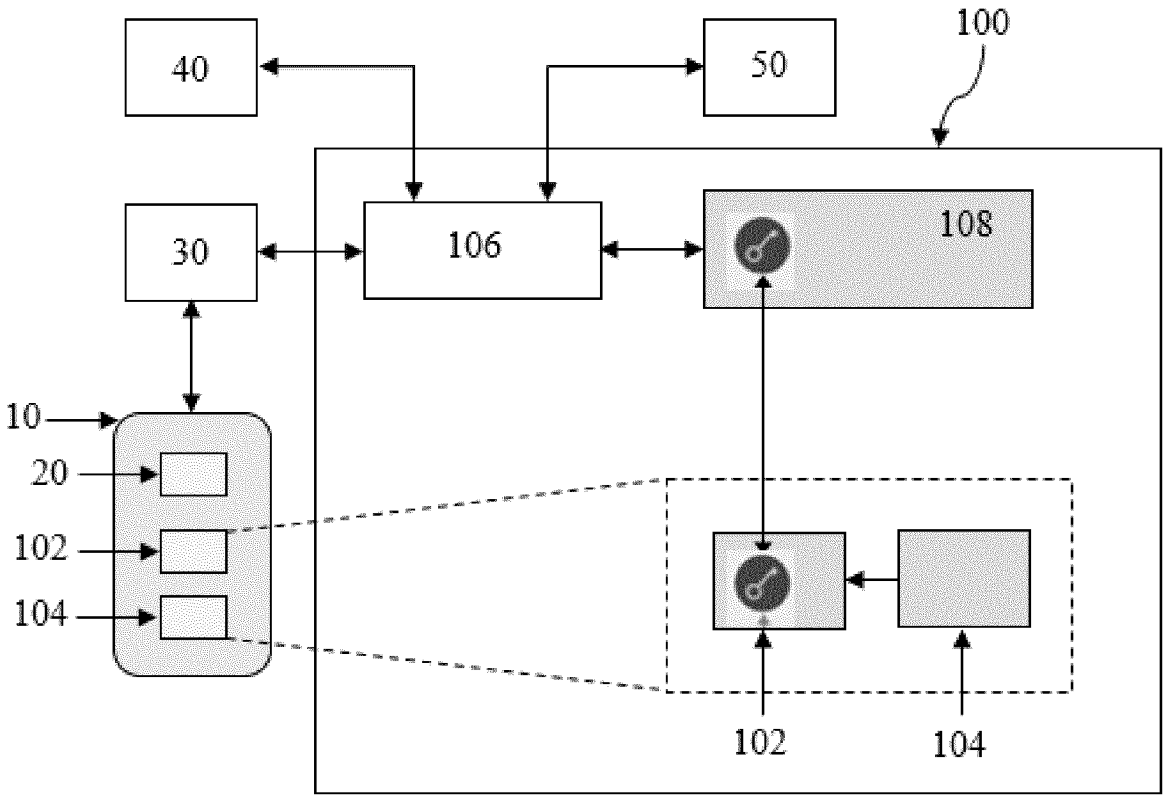
- механизм аутентификации (108); и

- центральный электронный коммутатор (106), выполненный с возможностью облегчать связь доверенного приложения (104), инструмента PSP (20) и сервера PSP (30) с механизмом аутентификации (108) и множеством серверов банковской системы (40, 50) для предоставления возможности зарегистрированному пользователю:

- регистрировать и создавать счет UPI lite для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций;

- зачислять деньги на созданный счет UPI lite с зарегистрированного финансового счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения; и

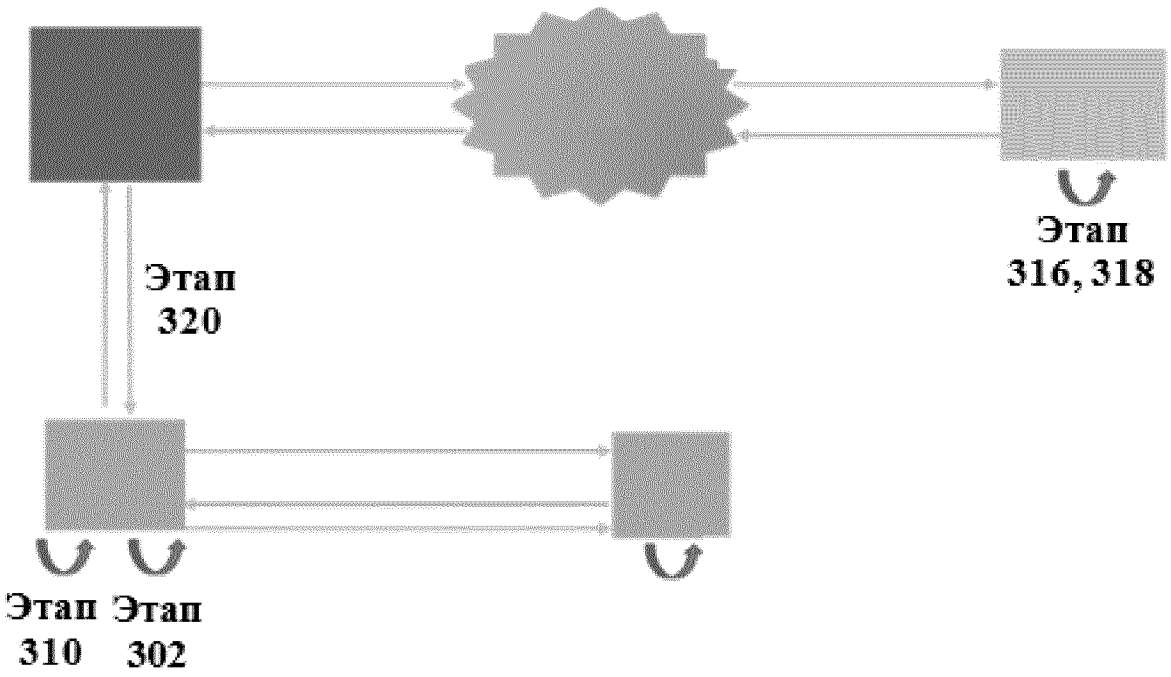
- использовать балансовую стоимость для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банковской системы (40, 50).



Фиг. 1


200
Выполнение, инструментом PSP, установленным на электронном устройстве, связанном с зарегистрированным пользователем, доверенного приложения в безопасной области хранения электронного устройства
202
Предоставление возможности, через центральный электронный коммутатор, доверенное приложение, инструмент PSP и сервер PSP осуществлять связь с механизмом аутентификации и множеством банковских систем для предоставления возможности зарегистрированному пользователю -
204
Регистрировать и создавать счет lite единого платёжного интерфейса (UPI) для выполнения основанных на правилах частично-онлайн и офлайн платежных транзакций
204a
Зачислять деньги на созданный счет UPI lite с зарегистрированного банковского счета, при этом стоимость денег, зачисляемых на счет UPI lite, хранят в виде балансовой стоимости в безопасной области хранения
204b
Использовать балансовую стоимость для выполнения частично-онлайн и офлайн платежных транзакций, не затрагивая серверы банка
204c

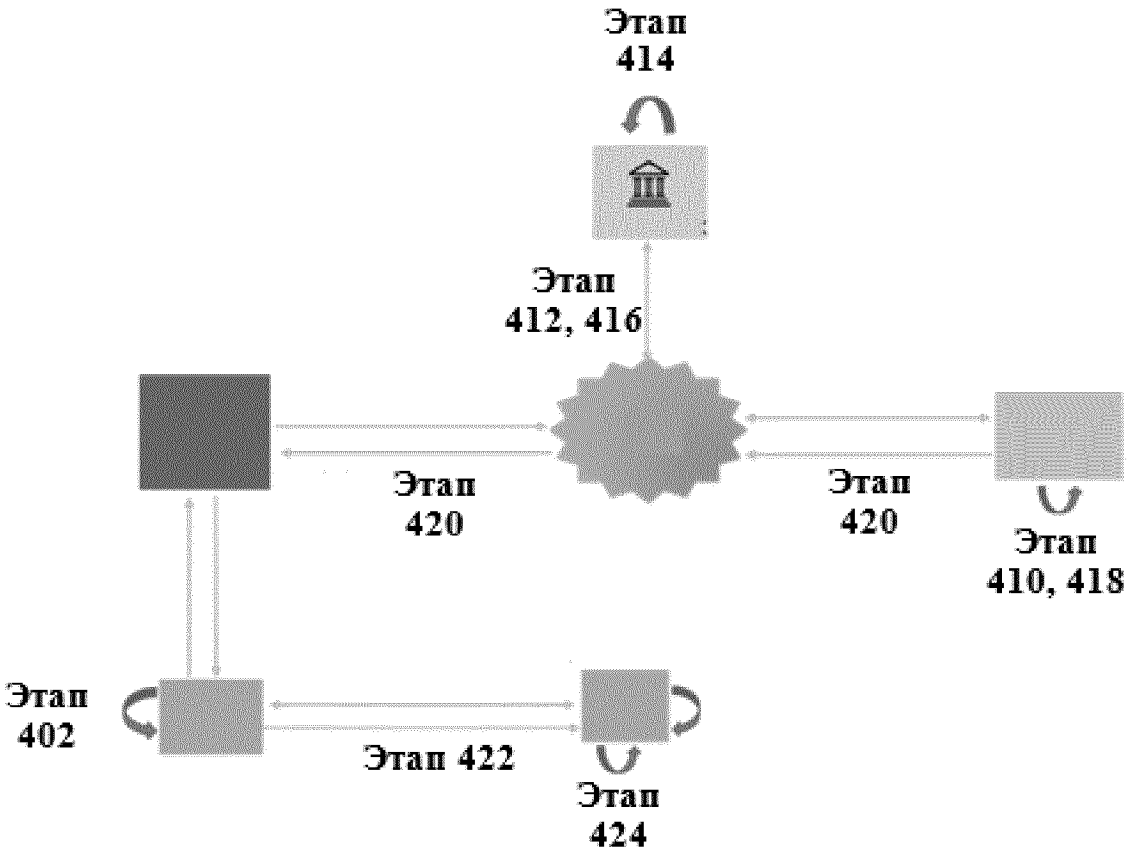
Фиг. 2



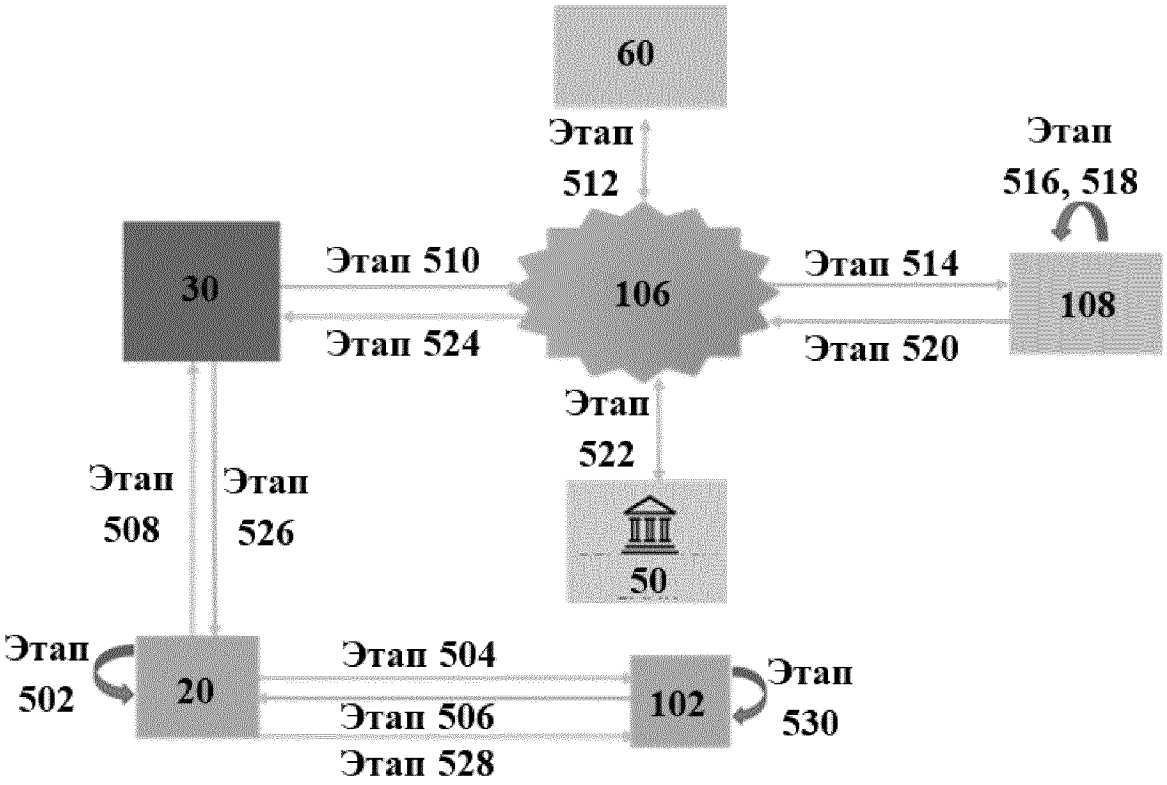
Фиг. 3

UPI-Lite Account
₹2.97
Balance as on 29 Aug '20
HDFC ****9829
UPI-Lite Account
Balance is low on your UPI Lite account
+ ADD BALANCE
Tap n Pay
BMTC | CCD Terminal ...
Auto Reload Settings
From: HDFC **** 5483
Generate Payment QR
Use this QR to pay offline
Transaction History
Last transaction on 28 Oct'20
Load Money
Please select the amount to load to the UPI-Lite account
HDFC ****9829
UPI-Lite Account
Load Amount
₹ 1000
PAY NOW
Juspay
9:41 AM
100%
HDFC Bank
UPI
ENTER UPI PIN
SHOW
1 2 3
4 5 6
7 8 9
0
Money Added
Account Details
HDFC ****9829
UPI-Lite Account
Balance: ₹1002.97
GO TO HOME

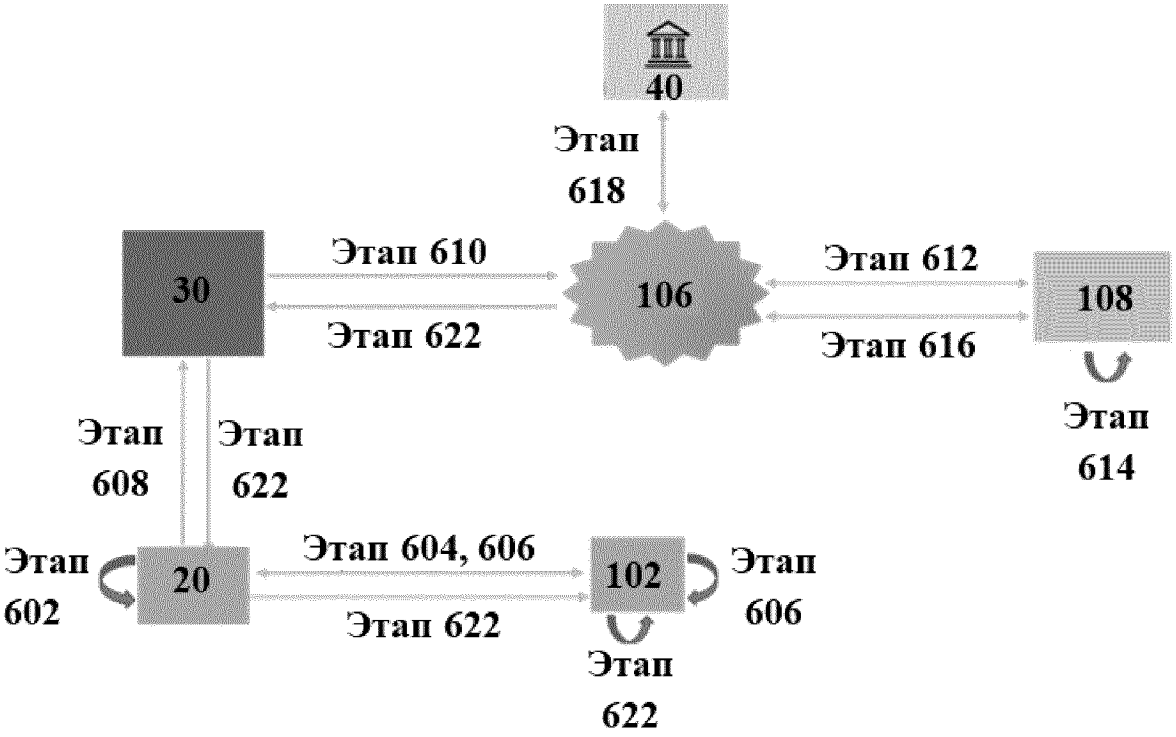
Фиг. 4A


Этап
414
Этап
412, 416
Этап
420
Этап
420
Этап
410, 418
Этап
402
Этап 422
Этап
424

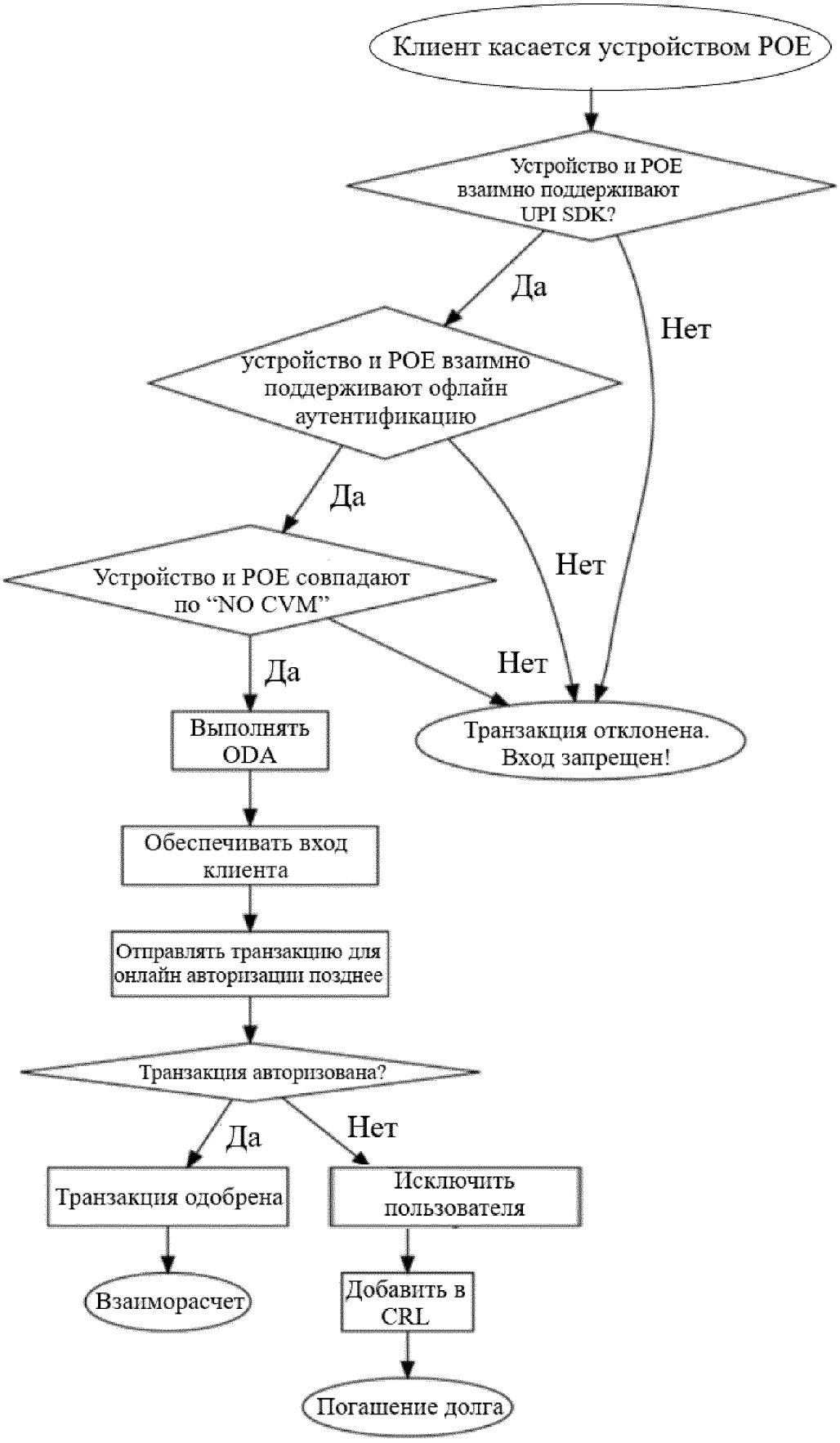
Фиг. 4B


60
Этап
512
Этап
516, 518
30
Этап 510
106
Этап 514
108
Этап 524
Этап 520
Этап
522
Этап
508
Этап
526
50
Этап
502
20
Этап 504
102
Этап
530
Этап 506
Этап 528

Фиг. 5


40
Этап 618
30
Этап 610
Этап 622
106
Этап 612
Этап 616
108
Этап 614
Этап 608
Этап 622
Этап 602
20
Этап 604, 606
Этап 622
102
Этап 606
Этап 622

Фиг. 6


Клиент касается устройством POE
Устройство и POE взаимно поддерживают UPI SDK?
Да
Нет
устройство и POE взаимно поддерживают офлайн аутентификацию
Да
Нет
Устройство и POE совпадают по “NO CVM”
Да
Нет
Выполнять ODA
Транзакция отклонена. Вход запрещен!
Обеспечивать вход клиента
Отправлять транзакцию для онлайн авторизации позднее
Транзакция авторизована?
Да
Нет
Транзакция одобрена
Исключить пользователя
Взаиморасчет
Добавить в CRL
Погашение долга

Фиг. 7